Mobility requirements in tactical IP networks

A study of available techniques and future challenges

Christian Wallin
Abstract

Mobility requirements in tactical IP networks, a study of available techniques and future challenges

Christian Wallin

This report studies the requirements of IP mobility in tactical networks. What challenges are there and how can they be dealt with. Different mobility aspects are studied and the challenges for these are presented and discussed. Within the report three different protocols namely Session Initiation Protocol (SIP), Mobile IP (MIP) and Host Identity Protocol (HIP) are evaluated and different implementations of these protocols are studied. A combination of MIP and SIP is suggested to solve mobility challenges in a tactical IP network that consists of multiple nodes with different properties. Currently unsolved challenges are discussed and a proposal for further work is presented.
# Table of Contents

ABSTRACT .......................................................................................................................... II

TABLE OF CONTENTS ................................................................................................. III

POPULÄRVETENSKAPLIG SAMMANFATTNING....................................................... V

DEFINITIONS ............................................................................................................. VII

ABBREVIATIONS / ACRONYMS ............................................................................. VIII

1 INTRODUCTION ........................................................................................................... 1

1.1 OPENING ................................................................................................................. 1

1.2 THESIS GOAL ........................................................................................................ 1

1.3 LIMITATIONS ......................................................................................................... 1

1.4 METHOD .................................................................................................................. 1

1.5 MOBILITY EXPLANATION .................................................................................. 2

1.5.1 User Mobility .................................................................................................... 2

1.5.2 Node Mobility ................................................................................................... 2

1.5.3 Session Mobility ............................................................................................ 2

1.5.4 Network Mobility ......................................................................................... 3

1.5.5 Service Mobility ............................................................................................ 3

1.6 NETWORK REQUIREMENTS ................................................................................ 3

1.6.1 Independence Requirement ......................................................................... 4

1.7 MOBILITY CHALLENGES .................................................................................... 4

1.7.1 Detection .......................................................................................................... 4

1.7.2 Reach-ability and Connectivity .................................................................... 4

1.7.3 Authentication and Authorization ................................................................. 5

1.8 SCENARIO DESCRIPTION .................................................................................... 5

1.8.1 Semi-Mobile Nodes ...................................................................................... 6

1.8.2 Mobile Nodes .................................................................................................. 7

1.8.3 Highly Mobile Nodes .................................................................................... 7

2 BACKGROUND .......................................................................................................... 8

2.1 SUMMARY OF PREVIOUS WORK ....................................................................... 8

2.2 DESCRIPTION OF PROTOCOLS ........................................................................ 8

2.2.1 Mobile IPv6 (MIPv6) ...................................................................................... 8

2.2.1.1 Network Mobility (NEMO) ...................................................................... 9

2.2.1.2 Hierarchical Mobile IPv6 (HMIPv6) ..................................................... 9

2.2.2 Host Identity Protocol (HIP) ......................................................................... 9

2.2.2.1 Host Identity Protocol based Mobile Router (HIPMR) ..................... 10

2.2.3 Session Initiation Protocol (SIP) .................................................................. 10

3 DISCUSSION .............................................................................................................. 12

3.1 WHY USE MOBILITY AT THE IP-LAYER? ...................................................... 12

3.2 COMPARISON OF PURE PROTOCOL IMPLEMENTATIONS ......................... 12

3.2.1 Protocol Performance ............................................................................... 12
## RESULTS .......................................................... 16

4.1 TEST DESCRIPTION ................................................. 16
4.2 FIRST SCENARIO .................................................. 16
   4.2.1 Test Setup .................................................. 16
   4.2.2 Test Results ................................................ 17
   4.2.3 Evaluation of Test Results ............................... 18
4.3 SECOND SCENARIO ............................................... 19
   4.3.1 Test Setup .................................................. 19
   4.3.2 Test Results ................................................ 19
   4.3.3 Evaluation of Test Results ............................... 20

## CONCLUSIONS .......................................................... 21

5.1 PROPOSED SOLUTION ............................................. 21
   5.1.1 User Mobility ............................................. 21
   5.1.2 Node Mobility ............................................. 21
   5.1.3 Network Mobility .......................................... 22
   5.1.4 Performance ............................................... 22
   5.1.5 Deployment ............................................... 22

## FUTURE WORK .......................................................... 24

6.1 REAL SCENARIO TESTING ......................................... 24
6.2 FURTHER DEVELOPMENT OF NETWORK MOBILITY .......... 24

## REFERENCES ........................................................... 25

APPENDIX ................................................................. A

1. MIP AND SIP ......................................................... A
2. MOBILITY ILLUSTRATIONS ....................................... B


Mobilitet kan även delas in i olika typer som ofta måste löses med olika metoder. I denna rapport diskuterar mobilitet av användare, noder, tjänster, nätverk och sessioner. När man pratar om mobilitet av en användare menar man att en användare ska kunna flytta sig mellan olika noder och att användaren ska ha samma rättigheter och resurser oavsett vilken nod denne använder och att andra noder fortfarande ska kunna nå denna användare efter en förflyttning. En nod ska kunna flytta sig mellan två fysiska platser och kunna byta anslutning till ett nytt nätverk utan att pågående sessioner påverkas och andra noder måste kunna kontakta noden efter förflyttning. En session ska även kunna flyttas mellan två användare utan att sessionen påverkas. Om flera sammanslutna noder rör sig samtidigt, t.ex. en buss fyld med passagerare som använder laptops, så vill man undvika att varje passagerare ska behöva hantera mobiliteten individuellt. Istället vill man att bussen ska kunna
hålla koll på nätverkets mobilitet och att alla passagerare inte ska behöva bekymra sig om bussens nuvarande position.

Rapporten utreder även vad man bör arbeta vidare med för att få en fullt fungerande lösning.
## Definitions

<table>
<thead>
<tr>
<th>Node</th>
<th>An entity of the network. Refers to a physical device such as a computer, VoIP phone, router etc, with at least 1 IP-address.</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>A person using a node or a service</td>
</tr>
<tr>
<td>Service</td>
<td>A resource supplied by a node or a user. This means a service that supplies, for example, VoIP or geographical information to another node or the user of a node.</td>
</tr>
</tbody>
</table>
### Abbreviations / Acronyms

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MIP</td>
<td>Mobile IP</td>
</tr>
<tr>
<td>HMIP</td>
<td>Hierarchical Mobile IP</td>
</tr>
<tr>
<td>HA</td>
<td>Home Agent</td>
</tr>
<tr>
<td>MN</td>
<td>Mobile Node</td>
</tr>
<tr>
<td>CN</td>
<td>Corresponding Node</td>
</tr>
<tr>
<td>CoA</td>
<td>Care-of Address</td>
</tr>
<tr>
<td>SIP</td>
<td>Session Initiation Protocol</td>
</tr>
<tr>
<td>URI</td>
<td>Uniform Resource Identifier</td>
</tr>
<tr>
<td>HIP</td>
<td>Host Identity Protocol</td>
</tr>
<tr>
<td>HIT</td>
<td>Host Identity Tag</td>
</tr>
<tr>
<td>RvS</td>
<td>Rendezvous Server</td>
</tr>
<tr>
<td>NEMO</td>
<td>Network Mobility</td>
</tr>
<tr>
<td>VoIP</td>
<td>Voice over IP</td>
</tr>
<tr>
<td>RTT</td>
<td>Roundtrip time</td>
</tr>
<tr>
<td>OSPF</td>
<td>Open Shortest Path First</td>
</tr>
<tr>
<td>AODV</td>
<td>Ad hoc On-Demand Distance Vector</td>
</tr>
<tr>
<td>OLSR</td>
<td>Optimized Link State Routing</td>
</tr>
<tr>
<td>DSR</td>
<td>Dynamic Source Routing</td>
</tr>
<tr>
<td>IETF</td>
<td>The Internet Engineering Task Force</td>
</tr>
</tbody>
</table>
1 Introduction

1.1 Opening
Since the nature strives for disorder it should be natural that also IP-networks should strive to handle networks of higher entropy. Two nodes should be able to reach each other at all times even when both are moving freely and independently. If the nodes are humans in a next generation tactical network then they should be able to share a wide variety of data and services. A military officer should be able to monitor the geographical position of every single entity in a military scenario. A soldier should be able to establish a video or voice session to any other soldier and keep the session alive and usable while changing position and attachment to the rest of the network. There should be no scalability issues of the network and every part of the network need to be autonomous. For the network to be functional and deployable it is essential to minimize the deployment cost and limit the amount of overhead data.

1.2 Thesis Goal
The goal for this thesis is to evaluate the currently available mobility protocols. What challenges can be solved with the available protocols and what challenges need future work to be solved. The thesis will present a suggested architecture to solve as much of the mobility challenges as possible in a given scenario. There will be a study of where in the network to put different required elements to gain mobility in the whole network and the independence needed within each network.

1.3 Limitations
This report will focus on the next generation networks where the standard protocol is IPv6 and thus any solution based on the requirement of an IPv4 network will not be discussed. There will also not be any detailed discussion of the security aspects of the network. Another limitation of the report is that it will not discuss how to solve any ad-hoc routing. Instead the work in this report assumes that there exists a working ad-hoc routing protocol.

1.4 Method
The writer of this report have to find standardization documents for a number of different protocols that could be used to achieve the goal of the thesis. These protocols have to be studied in detail and conclusions about how well suited they are have to be drawn. There is also a great need to study reports of implementations and tests of the standard protocols and implementations of any modification of the protocols that could help to solve the mobility for a given scenario.

There is also a need to simulate to point out any implementation disadvantages that could be hard to determine from the protocol descriptions and to determine certain aspects of the protocols such as delay in a scenario with numerous of nodes. It is good to make simulations to increase the
understanding of the scenario, the challenges and the implementation of the studied protocols. It was planned to also make tests on real hardware but the simulations were more challenging than expected so this went out of the scope of this report.

1.5 Mobility Explanation
Mobility in IP-networks involves many different scenarios and corresponding challenges. The following mobility types will be discussed in this report [1]:

- User Mobility
- Node Mobility
- Session Mobility
- Network Mobility
- Service Mobility

1.5.1 User Mobility
User mobility can be described as the movement of a user from one node to another i.e. by changing workstation. The users are required to access the same resources regardless of where they are. Every user needs to be able to contact other users irrespective of where they are attached to the network.

1.5.2 Node Mobility
Node mobility could be explained as a node that moves from one location to another and within this report it is assumed that the node have to change the IP-address. This will also often result in other types of mobility depending on what the node is doing during the movement.

There is also one kind of node mobility where a mobile node moves within a network domain where there will be no need to change the interface address of the moving node. This type of mobility will be solved by routing protocols. Either by a widely used routing protocol like OSPF or by ad-hoc routing protocols such as AODV, OLSR and DSR. A routing protocol made to handle a relatively static network such as OSPF will not be able to handle a network where the nodes constantly moves and updates their relations. In such a case one would want to use an ad-hoc routing protocol instead. These protocols are much better suited to handle frequent changes in the network topology. This report relies on the existence of a working routing protocol, thus solving the mobility of a node within a network domain without the change of addresses will not be discussed herein. There is an example picture of the two different types of node mobility in Appendix 2.

1.5.3 Session Mobility
This mobility involves the movement of an active session from one location to another. A voice call could be transferred during the movement of a node from one point of attachment to another in the network or from one user to another.
1.5.4 Network Mobility

Just like the name implies is this mobility a moving network consisting of multiple nodes. There is an example picture of this mobility in Appendix 2. In an IETF draft [2] three different approaches to handle network mobility are defined:

“Approach-1: A simplistic approach is to forget that there is a moving network and consider the moving nodes as separate mobile nodes. Each of the mobile nodes takes care of mobility signaling separately. The problem with this approach is that it leads to high amounts of signaling and long hand-off reaction times.

Approach-2: A tunneling approach is to create a tunnel from the Mobile Router in the mobile network to some home router in the fixed network side. All traffic is routed through this tunnel, making the mobile network to appear at a fixed location. The problems with this approach are suboptimal routing (so called triangular routing) and the larger packet size caused by tunneling overhead.

Approach-3: A third approach is to make the mobile nodes to delegate the right to do mobility signaling to the mobility router, which under certain conditions may delegate this right further into some node in the fixed network side. This draft presents a variant of this approach.”

1.5.5 Service Mobility

Service mobility is the movement of a service from one physical node to another. This mobility can be combined with session mobility meaning that any active session attached to a service is moved together with the service.

1.6 Network Requirements

All nodes should be able to communicate with each other and host different services that should be accessible by any node in the network. Every level of the network should be able to authenticate and authorize new nodes connecting to that level without the requirement of a connection to a higher or lower network. The networks will however not be required to authorize any new nodes to connect to a higher level network since the higher layer is assumed to handle this. When a node is moving around between networks it is important that it always can be reached. It is also important to minimize any delay and jitter that can occur when a node is moving around. The delay has to be small enough to maintain connectivity in active sessions and always maintain the quality of the service session, i.e. voice or video, without interrupting it when mobility occurs.
1.6.1 Independence Requirement
Every part of the network needs to be independent of other entities in the network. The reason for this is that the network should be able to operate in a tactical military scenario where every node and connection between nodes is vulnerable to attacks. Greater parts of the network will be very mobile without any guaranteed connection to other parts of the network. This makes solutions involving a single point of failure or solutions that require a connection to certain nodes inappropriate. Thus network services such as DNS or SIP need to be deployed on every independent level of the network so that the nodes therein can reach each other and also be able to interact with new accessing nodes.

1.7 Mobility Challenges
One of the major disadvantages today is that an IP-address is used as both an identifier and an address of a node. The IP-address is the name of a node and also used to route an IP-packet to the right destination. If a node is attached to a new network it will also need a new IP-address corresponding to the new position of the node. Since the IP-address is also used to identify that moving node, changing its IP-address will result in a new identity for the moving node. If instead the IP-address is left unchanged the packets would arrive to the nodes previous attachment without any receiver resulting in a lost packet.

1.7.1 Detection
The first challenge with node mobility is to detect the movement from a network to another i.e. moving away and lose connection with one access-point and move in range and connect to a new access-point. When a node is in range of multiple access-points clever decisions has to be taken for when to drop the current connection and start establishing a connection with a new access-point. Another challenge could be to detect that one of a node’s multiple connection interfaces is gained or lost i.e. a computer with a fiber and satellite connection loses one of the connections either because one of the connections loses connectivity by moving out of range or simply failing.

1.7.2 Reach-ability and Connectivity
Some movement will require the node to acquire a new IP-address. In IPv4 this has to be preconfigured manually, by assigning a static IP-address to a node, or by some kind of DHCP service, which dynamically can assign a new IP-address for any connecting node. The dynamic address assignment can in IPv6 be solved by stateless address auto configuration. This change of IP-address has to happen without losing any current or upcoming connections. As a result some action has to be taken to inform upcoming connections about the change of location.
1.7.3 Authentication and Authorization

Any new nodes accessing a network have to be authenticated to verify who the new node is and also authorized to be allowed to use different services.

---

1.8 Scenario Description

The network that will be analyzed consists of a number of different nodes with different levels of connectivity to each other and with various capabilities. Each level of the network will be described in detail within this chapter. There will be one or more stationary core networks, such as a military base, with a very high bandwidth and low latency connection to other networks including the Internet.
1.8.1 Semi-Mobile Nodes

There will be several nodes that will connect to these core networks. These nodes will be semi-mobile in the way that they will not have connectivity while moving and they will be stationary during their connection to the different core networks. The capacity of the network connection can vary from high latency connection such as a satellite connection to a very high bandwidth connection with low latency such as a fiber connection. Different nodes on this level will have no direct connection to each other.

2 - Example of how the radio coverage of the nodes could look like. The stationary and semi mobile nodes have a point to point connection between them and the semi mobile nodes and two of the mobile nodes have a point to point connection. The mobile nodes have a radio connection between them with a large range and the highly mobile nodes have a low range radio connection between them.
1.8.2 Mobile Nodes

There will be groups of mobile nodes forming ad-hoc networks connected to one of the semi-mobile networks. The bandwidth available will be a wireless network connection with high bandwidth and low packet loss. These nodes should be able to move around inside their own network and they should also be able to move to another network of the same type. The mobile ad-hoc network should also be able to move to another semi-mobile connection point, within the current core network, without interrupting any ongoing sessions and also move to another core network without any live session. New authorized mobile nodes should also be able to connect to this network.

1.8.3 Highly Mobile Nodes

Below the mobile ad-hoc network another ad-hoc network is attached. There will be more movement within this level of the network. The nodes on this level will have very limited resources. The connection between these nodes will be a wireless connection with limited bandwidth. They will have limited battery capacity and the computational performance will be low. These highly mobile nodes should also be able to move around inside the ad-hoc network, change ad-hoc network and the whole ad-hoc network should be able to change its point of attachment to another mobile node during a live session. Another mobile node should be able to be authorized and connect to this network even when the ad-hoc network has no connectivity to a mobile node.
2 Background

2.1 Summary of Previous Work
There is a lot of work in progress concerning Mobility in IP-networks. The IETF working group has published numerous of different approaches to solve different type of mobility challenges, Mobile IPv4, Mobile IPv6, Host Identity Protocol and Site Multihoming by IPv6 Intermediation all with different extensions.

Försvarets Materielverk, FMV (Swedish Defence Materiel Administration) have published a Design Rule for Mobility [3] with underlying documents covering Mobility in IP-based systems where the general use of mobility protocols has been studied.

Former reports from FMV [1] argue in favor of placing mobility support in the IP-layer.

2.2 Description of Protocols

2.2.1 Mobile IPv6 (MIP6)
Mobile IPv6 is developed to solve mobility challenges of mobile nodes. Everyone contacting the mobile node will always use a static IP-address corresponding to the address space of the home network of the mobile node. In the home network a Home Agent, typically a router, will take care of all arriving packets and forward them to the current address of the mobile node. The mobile node will send update packets to the Home Agent as soon as the IP-address for the mobile node changes and the mobile node will also send a direct location update to all corresponding nodes which the mobile node have an active session with. [4] [5] [6]

Using the MIP6 protocol requires the mobile node to always be able to reach its Home Agent and the Home Agent need a static IP-address for this to be possible. If anything happens to the Home Agent the mobile node will be unreachable which make the Home Agent a single point of failure.

Another limitation of MIP6 is that it requires usage of IPv6. The basic MIP6 protocol also offers no verification of the identity of the nodes. [7] [8]
There exist a couple of different extensions to the basic MIP6 and all of interest to our scenario will be discussed in separate sections.

2.2.1.1 Network Mobility (NEMO)
There is a NEMO protocol extension to MIP6 [9] [10]. The protocol adds the possibility for a mobile node to be a mobile router. The router will tunnel traffic from the mobile router to its Home Agent and make any movement of the network transparent to nodes within the mobile network. The nodes within the mobile network will have a public IP-address belonging to the mobile routers home network. This will make them always reachable on their address even if the router changes its point of attachment.

In [11] requirements needed for a NEMO protocol is published and with those requirements fulfilled it would be very usable in our scenario. Unfortunately there is no known implementation of such a protocol.

2.2.1.2 Hierarchical Mobile IPv6 (HMIPv6)
Extending the MIP protocol to a hierarchical protocol could severely decrease the handover times for the protocol in certain scenarios. This protocol introduces a new entity called a Mobile Anchor Point (MAP). The MAP is typically a router somewhere closer to the Mobile Nodes (MN) current point of attachment. A MAP will announce its existence through router advertisement messages and by listening to these messages a MN could detect the existence of a MAP. The mobile node will register its Regional Care-of Address (RCoA) with the MAP and as long as the MN moves within the area of the MAP it will send binding updates to the MAP instead of the HA, which can reduce handover times severely if the MN is positioned far away from the HA. [12]

2.2.2 Host Identity Protocol (HIP)
HIP [13] [14] introduces a new namespace to separate the location from the identity of a node. It uses the normal IP-address for routing but also uses a Host Identity Tag (HIT) which is a hashed public key used to identify a node. When someone want to reach a node using HIP on the internet the HIT will be used instead of the currently unknown IP-address of the mobile node. The mobile user will always be able to get reached since the HIT never change. To establish contact a HIT Domain Name System (DNS) is used which return the IP-address of the mobile node’s Rendezvous Server (RvS). This server stores the latest IP-address of the mobile node and this address is used to establish a connection with the mobile node. For this to work the mobile node must update its address to the Rendezvous Server as soon as it change its IP-address. To avoid a single point of failure and add some protocol resilience, multiple RvSs could be used.
Each node needs to send a total of two packets to the corresponding node to establish a connection between two nodes. This is a way to authenticate the nodes and prevent them from several possible attacks. No contact with RvS needed after establishment. Update packets will be sent directly between end nodes as long as they do not move simultaneously, in which case they will have to contact each other’s RvS to get the new address of the other node.

HIP is transparent to the use of different IP versions since the HIT is used above the IP-layer and will therefore work well with both IPv4 and IPv6 networks.

The handover time can be decreased with Credit-Based Authorization which allows information to be sent between nodes before the base exchange is completed.

### 2.2.2.1 Host Identity Protocol based Mobile Router (HIPMR)

This is a protocol extension to support NEMO for the HIP. A mobile node will setup a connection with a corresponding node just like it would do in normal HIP. A mobile node will monitor router advertisements and if a mobile node detects a mobile router it will do a HIP base exchange with the mobile router. After the base exchange is done a mobile node will send a key, for each active corresponding node with an active session, to the mobile router. The mobile router can then use these keys to send location updates to the each corresponding node on behalf of the mobile node if the mobile router changes its point of attachment. This will make the movement of the router transparent to the nodes within the network. Applying this technique instead of letting each node send its own location update will save bandwidth in the network, especially if the network has multiple layers of mobile sub-networks (a multilayered network). [2]

### 2.2.3 Session Initiation Protocol (SIP)

SIP [15] is an application layer protocol in the TCP/IP stack model and a Session Layer protocol in the OSI stack model made for session handling, typically used to setup video and voice sessions. When using SIP to set up a session between two user agents a uniform resource identifier (URI) will be used as address of the node to start a session with. The URI could be seen as the IP-address of a user but instead of a hard to remember, combination of numbers, an identifier like “firstname.lastname@association” is often used. An “INVITE” will be sent to the corresponding IP-address of the URI, which will...
respond with an “OK” message that the inviter later will send an acknowledgment message, “ACK”, of. After this SIP is done and the media stream between the nodes can start. As soon as a session is initialized all data between the nodes will be sent directly between the nodes.

Because of the URI a user can move between different nodes and still be reachable by any other node. The node only has to update the URI->IP binding when changing his point of attachment.

If one node acquires a new IP-address during an active session with another node he can send a “re-INVITE” message containing his new IP-address to the node and they can continue the session using the new IP-address. This handover could result in seamless mobility if the node that acquires a new IP-address will be reached also on its old IP-address long enough for the new “INVITE” message to reach the other node.

SIP is the session handling protocol used by the Swedish military and it is being implemented in a new communication node called KomNod which is going to be used in the next generation military network.
3 Discussion

3.1 Why use Mobility at the IP-Layer?
As been motivated in [1] mobility should be solved at the lowest possible layer of the network stack and the lower bound is set by the address space. In the previously described scenario only IP-addresses can be used to reach all nodes and thus the IP-layer is the lowest possible layer which can fully handle node mobility. Some of the reasons to choose the lowest possible layer are to minimize overhead and keep as much of the stack as possible unaware of the existence of mobility. This will ease the creation and implementation of overlaying protocols.

3.2 Comparison of Pure Protocol Implementations
There are many protocols discussed in previous sections of the report and there is a need to study how well the protocols perform in a simulated or emulated environment.

3.2.1 Protocol Performance
[16] is a performance test of MIPL 1.1 on Linux 2.4.26. MIPL1.1 is an implementation of standard MIP6 for Linux. The test shows different delays for an implementation of MIP6, without any extensions to the protocol. The delays discussed is the delay when a mobile node move from its home agent to a foreign network, the delay when the mobile node move from one foreign agent to another foreign agent and finally the delay when the mobile node move back to its home agent.

Different proportion of node movements were set up but all resulted in the same delays for the different mobility types. The first movement resulted in a delay of 1.15s, the second movement resulted in a delay of 0.17s and the third movement resulted in a delay of 0.10s. The RTT is less then 1ms between two nodes in the scenario.

In [17] a mobile node will move randomly inside an area of nine access-points, requiring the mobile node to change IP-address. The result shows that the number of lost packets and the handoff latency could be lowered severely with HMIP if the RTT to the HA is increased. This means that HMIP would outperform standard MIP if the Mobile node is moving far from the home agent.

![Diagram of 9 access-points](image)
3.3 Cell Switching

Another interesting challenge to deal with is when to switch network when multiple access-points are in range. The two basic ways to do this is either change as soon as you gain a new network connection, called eager cell switching, or not to change unless you lose the previous, called lazy cell switching. As shown in the pictures below the different strategies have their advantages for different node movement scenarios. Since the node will experience handoff latency when the node is unreachable it is very important to make the right decision for each scenario to avoid unnecessary packet loss. [18]

A work around for the challenge with cell switching could be the usage of dual-links. This meaning that a node has two wireless interfaces. The node will setup up a connection with an access-point just like the normal case. Then when a new network connection is detected the second wireless interface will begin handoff with the new access-point while the first interface keeps the current connection. Then one interface could use eager cell switching to setup a possible new connection while the other interface keep implement lazy cell switching and keep the current connection until it is lost. By doing this a seamless handover could be acquired where the handoff delay is non-existent and no packets will be lost in the transition between two access-points. [19]

Even if it is possible to achieve seamless handover with dual-links it is also needed to minimize the handover delay as much as possible. There are several reasons to reduce this delay. When a node moves fast or when the networks is not overlapping very much the handover delay is very critical. The delay can be lowered in several ways. By letting the access-points take care of the CoA address generation and duplicate address detection, instead of the mobile node, and start these layer 3 operations based on layer 2 triggers the handover delay can be cut down from half to less than a third of the time of standard MIP. [20] There is also possible to reduce the delay even further by having topology aware nodes in the network that share information with the mobile node. With shared topology information and the knowledge of the mobile node’s direction of movement the next access-point can be predicted and the handover delay could be reduced enough to only lose few packets down to even zero packets lost. [21]
Studies have shown that the usage of optimistic duplicate address detection could reduce the handover delay related to the, by Mobile IP, recommended determination of the uniqueness of an address. [22]

### 3.4 Unsolved NEMO Challenges
There exists no complete and mature solution to solve the challenge with a moving network. Currently the only fully working solution would be to let all nodes in the moving network to take care of their own address and all nodes have to updated their own address when the access-point change its address. There have been work in both MIP and HIP working groups to solve the challenges. The solution that is most mature is the MIP solution where a tunnel from the moving access-point to its HA is setup and all traffic from within the network is tunnel through the HA. This has not been tested enough and it also has a lot of scaling disadvantages since it adds unnecessary delay from triangular routing and the tunneling overhead could considerably increase the packet size of voice packets or other small packets in a large multi-layered network. The solution for HIP delegates the update rights from the nodes within the moving network to the access router so that it does update on behalf of all nodes in the network. This limits the traffic in the network and does not add any tunneling overhead or triangular routing but has so far only been seen in a draft.

### 3.5 Evaluation of Combined Protocols
Pure protocol implementations are not working well enough for large scale networks where various types of mobility are required together with the requirement of seamless handover, as could be seen in the previous chapter. In this chapter a combination between different protocols will be studied and evaluated in search for a more complete solution. The protocols that will be examined are combinations of SIP, MIP and HIP. SIP is currently the only available protocol to solve user mobility without the need of assigning a hard to remember IP-address or a HIT to each person. MIP and HIP both solves multiple other mobility issues and have been tested to work together with SIP as will be explained.

#### 3.5.1 SIP and MIP
Studies show that a pure SIP mobility solution is outperforming a combination of MIP and SIP where each protocol handles user and node mobility respectively. [23] This can easily be understood since both protocols have to send update information to its respective entity, adding extra traffic and delay. If instead of letting each protocol handle its own mobility an integration of the entities is done, then the signaling costs could be severely decreased. The full integration of the SIP server and the functionality of the HA reduces the most signaling cost but there exist variants where the entities are only slightly modified to cooperate, which almost achieves as good as the full integration. [24] The first variant let the MIP HA handle the location of the mobile node and the SIP server use the HA as a location service. In the second alternative the MIP HA is sending an update to the SIP server when receiving a location update from the mobile node.
The advantages of using a combination of SIP and MIP to handle mobility are that both UDP and TCP traffic can be initiated, which is further discussed in chapter 5.1.2, and having multilayer mobility management both handles more mobility scenarios and can outperform the standalone versions. When the protocol is used to handle a VoIP session it can take the advantage of the well developed session handling of SIP together with the fast update property of MIP. This result both in less jitter and average end-to-end delay of a voice session. [25]

3.5.2 SIP and HIP
Integration between SIP and HIP (SHIP) has in simulations outperformed protocols where SIP and MIP are working side by side. [26] However there is no known test that compares SHIP to the integrated SIP and MIP scheme. Many applications could benefit from the added security of HIP since all traffic is IPsec protected in HIP. But RTP applications will suffer from the added overhead that comes with IPsec. Other positive things that come with the usage of HIP is the ability to implement multihoming and the usage of HIT as peer ID adds a security binding between identities and peer ID’s. [27]
4 Results

4.1 Test Description

All tests are performed in Opnet Modeler, which is network simulation program, and the version used is 11.5. This program make it possible to build your own node models but all nodes used in these simulations are made from standard models with some minor configurations made to the standard models to support Mobile IPv6. All scenarios have a voice application running between at least two different nodes. This voice application is a standard application definition called “IP Telephony” which uses the G.729 voice encoder.

4.2 First Scenario

This scenario was built to show how the performance of a highly mobile network could be increased by adding a protocol which could handle node mobility. Unfortunately some limitations with Opnet was discovered which prevented the implementation of MIP for this scenario. Instead this scenario is made only to show the performance of a network with mobile nodes without any protocol that handles the mobility for the nodes.

4.2.1 Test Setup

The first scenario consists of 7 wireless routers called “wlan2_router_adv”, which each is an access-point hosting a network for 5 wireless workstations called “wlan_wkstn_adv” on one wireless interface and the routers have another wireless interface with which the routers communicate between each other. All nodes use the AODV AD-HOC routing protocol with standard settings. There are no nodes with any MIP settings configured.

In the network there are 8 nodes using a two-way...
voice application in pairs namely:

- MN_1_3 <-> MN_3_4
- MN_2_3 <-> MN_5_5
- MN_4_4 <-> MN_7_3
- MN_6_1 <-> MN_7_2

Each node is only able to communicate with other nodes in the same sub-network or with the access-point of the same network. Meaning MN_3_1 can talk directly with AP_3 or MN_3_4 but to be able to talk with MN_4_3 the traffic must go through both AP_3 and AP_4.

In the first test all nodes will be stationary, in the second test all workstations will move in a random pattern, using the built-in “Random Mobility Profile”, choosing a destination point and move there and then pick a new destination, and in the third test also the access-points will be moving in the same random pattern.

### 4.2.2 Test Results

The pictures below show how much traffic each of the nodes with an active voice communication receives during the scenario. The first picture shows the traffic for the test where no nodes are moving and the second picture shows the traffic for the test where all nodes are moving around.

![Traffic received for nodes with an active voice communication in the test where no nodes are moving. Each node is always transmitting 1000 bytes/s and the nodes also receiving 1000 bytes/s have a voice communication without any interruption. Sometimes the traffic received is dropping and then increasing right after which indicates a delay of the traffic.](image)
4.2.3 Evaluation of Test Results

In the test where no nodes are moving all traffic is received by each node with a very small variation of the delay. This is the desired behavior of a voice communication. In the second test several packets are lost because of the nodes moving out of range of their access-point and without any configured protocol to handle mobility this will most probably happen. The voice communication will suffer from the lost packets and the communication between the nodes will be interrupted.
4.3 Second Scenario
The problems with MIP in the first scenario resulted in this second scenario. This scenario was made to show how MIP could increase the performance of the voice traffic for the moving nodes in a simpler scenario. In this scenario the number of nodes is very limited and no workstations have any ad-hoc routing configured.

4.3.1 Test Setup
The second test suit consists of 2 routers called “wlan2_router_adv”, which each is an access-point hosting a network for 1 wireless workstation called “wlan_wkstn_adv” on one wireless interface and the routers have another wireless interface with which the routers communicate between each other. All routers use the OSPFv3 routing protocol with standard settings.

The wireless workstations have a two-way voice application running between them and one node will be moving around the two routers in a defined pattern where the node always should have connectivity with at least one of the two routers.

In the first test no node will be configured to handle mobility but in the second test the two routers will act as a MIP HA for the, at the start of the scenario, closest wireless workstation and the wireless workstations will have the route optimization flag enabled. The route optimization flag means that the nodes will send a binding update to the other wireless workstation when they change connection between the routers. This is done to avoid triangular routing resulting in that the traffic will be sent directly between the two nodes instead of always be tunneled through the HA of the nodes.

4.3.2 Test Results
The first picture displays the received voice traffic of a node when no MIP is configured for the scenario. The next picture show the traffic received when MIP is enabled for the moving node and the third picture shows a close-up of the received traffic when the node has to switch from one access-point to another.
4.3.3 Evaluation of Test Results

The results show that MIP could increase the performance of a voice session severely for certain scenarios. But the handover delay of the basic MIP protocol is still too large and multiple packets will be lost or severely delayed which would render them useless. This behavior will prevent the wanted seamless handover that is needed for high quality voice traffic to be fully functional.
5 Conclusions

5.1 Proposed Solution
The previous chapters provide numerous reasons and examples of limits with the existing protocols. Some solutions discussed within the report are better suited than others but there are yet no complete solution in this area of science. Thus there is a need to combine protocols to achieve a somewhat complete solution for the given scenario.

5.1.1 User Mobility
The first requirement to deal with is the user mobility requirement that requires a user to always maintain connectivity and for the user to be able to access different resources such as an email client or a voice user ID. As discussed in previous chapters the only really good way of dealing with this is to use the SIP protocol and assign a URI for each user. Then a user can update his location with a SIP server upon movement and everyone who wants to contact the user can always use the same URI since the URI for a user will not change upon movement. Thus introducing the URI will “remove” the node identifier property of an IP-address and the IP-address will be used only as an address of a node.

5.1.2 Node Mobility
SIP could also be used to handle node mobility. However this is not preferred due to the need to encapsulate the IP-packets and use a tunnel, which would increase the packet size and complicate any enforcement of quality of service, for any TCP traffic initiated by SIP. [28] Studies have shown that a pure SIP solution outperforms solutions where SIP and MIP coexist, illustrated in Appendix 1, when the scenario are limited to only UDP traffic being initiated. [23] But if the protocols are integrated to cooperate between each other, which would eliminate any redundancy from the dual location updates, they would outperform a pure SIP solution and the integrated solution would be able to initiate both UDP and TCP traffic. [29] [24]

The only mature protocols suited to work together with SIP are the HIP and the MIP protocols. Both have been tested to work together with the SIP protocol. However the maturity of MIP, with numerous of publically available simulated and emulated tests, exceeds the maturity of HIP and since reports have shown that the IPsec property of HIP, which require traffic tunneling, can reduce the performance of streaming sessions [27], one would go for MIP as the protocol to handle node mobility. There is a need of modifications to the MIP protocol to be fully integrated with the SIP protocol and the single point of failure disadvantage of standard MIP needs a workaround. Instead of using a normal HA one could use a distributed solution of Mobile IP such as [30] which should be more natural to integrate with the structure of the SIP protocol which is based on distributed location registrars.
5.1.3 Network Mobility
As described earlier in this report NEMO for MIP tunnels all information from a mobile access-point through the HA of the mobile access-point. This makes any mobility of the mobile access-point transparent to the nodes within the network because they can keep their IP-address which is a topology correct IP-address of the mobile access-point’s HA. However there will be no such static HA of any router in the proposed solution. This means that the normal NEMO for MIP cannot be applied and currently there exist no solution that handles NEMO for the proposed solution. Therefore each node of a moving network would have to deal with the mobility individually, meaning that all nodes would have to acquire a new IP-address if their access-point changes the network address and all nodes with an active session would have send an update all nodes with which the node have an active session with.

This is not a very good solutions since multi nested moving networks would require much more bandwidth then a solution where each mobile access-point handles the mobility for all nodes within the mobile sub-network. Therefore a better solution for this will be proposed as future work later in the report.

5.1.4 Performance
Integrations between MIP and SIP have shown to overall perform at least as good as the protocols one by one. However this is not good enough to realize the seamless mobility requirement as needed for streaming sessions such as VoIP to work. It is therefore very important to take further actions to minimize delay and jitter. There are many ways of reducing the delay such as limiting the amount of data that have to be sent during a handoff or by decreasing the distance a location update message have to travel to take effect. But to really achieve seamless mobility other measures such as layer integration also have to be taken into account. A solution that triggers layer 3 events when receiving information from a new access-point at layer 2 would be able to reduce the handover delay. One such implementation is the MIP Fast Handovers [31] protocol that has shown to achieve considerably faster handoffs compared to standard MIP solutions. [32]

An advanced algorithm that make intelligent decisions for when and if a handover from one access-point to the next access-point should happen also have to be developed as discussed in the previous chapter about cell switching. Using geographical information to predict the change of access-points could be helpful to achieve this which has been shown in [33].

Other things that need to be reduced during a handoff are the time it takes to configure a new address. As discussed earlier in this report the access-points could help out with the address configuration and the usage of optimistic duplicate address detection would reduce the configuration time. Any use of a service such as DHCP should be avoided because DHCP is relatively slow for address configuration compared to the stateless address auto-configuration of IPv6 [34].

5.1.5 Deployment
Every node need to hold SIP URI information of every other node there could be a need to set-up a voice session with. The reason for this is that the URI will be used as an identifier of a node and you
need to know who you want to contact when contacting someone. There will also be a need for
every node to have a SIP server in order to achieve maximum resilience or the SIP servers could be
spread over a number of nodes within each subnet. This SIP server need to store the current
mapping of SIP URI to IP-address for every URI the node, or group of nodes using that SIP server,
have. When a SIP server receives a new IP-address of a URI it should store that information in the
database and the SIP servers on each node need to share any new information to everyone with a
direct connection. The information shared could be very limited and need only to contain any new
information. If the SIP server information will be spread fast all nodes should be able to establish a
new session with any moving node within reasonable time. The location updates to the SIP server
should be sent using MIP updates since the SIP and MIP servers are integrated as one entity. As soon
as a session is setup between two nodes MIP with route optimization should be used between them
eliminating any need to contact other nodes for location updates. This would result in a maximum
downtime of one RTT between the nodes. If the nodes move simultaneous the update packets could
be lost and the nodes would have to establish a new SIP session between them.

16 - Illustration of the possible traffic flow between a Corresponding Host (CH), a Mobile Host (MH) and an
integrated SIP Server and Home Agent (SRV). CH ask the SRV for the address, to a given a SIP URI, which is
returned. Then CH send a session INVITE which is being acknowledged twice before the traffic can start.
After movement only a MIP Binding Update (MIP BU) will be sent from the MH and the MH also have to
register the new IP with the SRV using another MIP BU, that the server will send and Binding
Acknowledgment of (Back), so other new nodes can reach MH at the new
destination. The integrated SIP and MIP HA will share the location
information for the MH.
6 Future Work

6.1 Real Scenario Testing
At the time of writing this report there are so far no known real implementation of any combined protocols. There is not even any published test of an emulation of the combined protocols. These tests have to be done on real hardware rather than just simulated numbers to provide more solid results and to get a picture of how hard and time consuming the integration of the protocols would be. This would also help to identify any possible challenges with the integration of other protocols or hardware.

6.2 Further Development of Network Mobility
As discussed earlier there are three different approaches within IETF to handle network mobility. The proposed solution in this report suggests in the previous chapter that the current way to deal with network mobility would be to let all nodes handle their own mobility. This would result in heavy traffic upon a network movement that one would want to limit as much as possible.

The solution that MIP working group is working on suggests that the nodes of a mobile network would have a topology correct IP-address of the moving access-point’s home network. This would limit the traffic in the moving network but would also result in traffic overhead by tunneling data to the home network and this solution also suffers from the negative effects of triangular routing.

The third approach is the most promising solution that is currently work in progress by the HIP working group. As said earlier this solution would delegate the location update rights from the mobile nodes to the mobile access-point which would limit the traffic within the moving network without adding any additional load outside the network. This is however only a draft and is implemented within the HIP protocol which already suffers from the overhead of traffic tunneling. One would want to continue working on these different approaches towards a solution that would limit the update traffic without adding any other additional overhead.
7 References


1. MIP and SIP

17 - Illustration of the traffic flow between a Corresponding Host (CH), a Mobile Host (MH), a MIP Home Agent (MIP HA) and a SIP Server (SIP SRV). CH ask the SIP SRV for the address to a given URI which is returned. Then CH send a session INVITE which is being acknowledged twice before the UDP traffic can start and the TCP traffic is first tunneled by the MIP HA before the CH recieves a MIP Route Optimization Binding Update (MIP-RO BU), after which the TCP traffic can go directly from the CH to the MH.

After movement the same SIP procedure have to happen for the UDP traffic and the CH have to send a new BU to the CH for the TCP traffic to continue. The MH also have to register the new IP with the SIP SRV and also send a BU to the MIP HA so other new nodes can reach MH, with both TCP and UDP traffic, at the new destination.
2. Mobility Illustrations

18 - Node Mobility between two networks: Node (A) moves (1), looses the connection (2) and later establish a new connection (3) within a new network with a new IP-address of

19 - Node Mobility within a network: Node (A) moves (1), looses the connection with two nodes and later establishes a new connection (3) without that node (A) changing IP-address

20 - Network Mobility: A network (A) moves (1) and loose network connection (2) and later establishes a new connection (3)