Moving Networks in the IST-MIND Project

Csaba Simon[1], Gösta Leijonhufvud[2], Tapio Suihko[3], Philip Eardley[4], Attila Török[1]

[1]Budapest University of Technology and Economics, Hungary, {simon,torok}@ttt-atm.ttt.bme.hu
[2]Ericsson Research, Sweden, gosta.leijonhufvud@era.ericsson.se
[3]VTT Information Technology, Finland, tapio.suihko@vtt.fi
[4]BTexact Technologies, United Kingdom, philip.eardley@bt.com

ABSTRACT

This paper aims to present the results of the European IST project MIND on the mobility management of Networks in Motion, or Moving Networks (MONET). Nodes in MONETs move as a unit with respect to some frame of reference. The objective of the project is to facilitate the rapid creation of broadband multimedia services and applications that are fully supported and customised when accessed by users of future mobile systems ("beyond 3G"). The MIND network is itself fully IP-based, both in the sense of using IP transport internally, and using IP mechanisms to support terminal mobility and QoS. The authors identified the possible scenarios that involve the attachment of MONETs to the access network architecture specified in the project. The paper presents three scenarios to solve the support of MONETs. It also analyses the particularities of these three scenarios.

I. INTRODUCTION

With the spread of the new wireless broadband technologies soon all familiar wired network services and applications will be available in the vehicular environment, as well. These services range from typical Internet and office applications, like web-browsing to value added services like location-based information services. In order to facilitate this process the research community should provide solutions to hide as much as possible the details of mobility and access management involved in this type of communication.

Vehicular networking environments are modelled by Networks in Motion, or Moving Networks (MONET). By definition, nodes in MONETs move as a unit with respect to some frame of reference, which is in contrast to Mobile Ad Hoc Networks (MANETs) where the nodes move arbitrarily with respect to each other. A MONET may be composed of MANET nodes and a group of mobile nodes (i.e., a MONET) may move within a MANET. Because of this intertwining, the problem area easily becomes convoluted. Therefore, we focus on scenarios where the nodes in the MONET do not form a MANET and the MONET is connected directly to the wired access network elements.

The problems in and requirements for MONETs are investigated in IETF's NEMO WG [1]. In the IETF, the reference protocol for mobility management is Mobile IP [2]. Here we discuss how MONETs could be adapted to the MIND architecture, which deploys a hierarchical mobility protocol.

Vehicular Moving Networks are also researched in IST DRIVE [4], and its follow-up OverDRiVE projects [5], with special focus on cars and Mobile IPv6 [6]. MIND [7] tried to serve a larger number of moving nodes and it used the hierarchical mobility approach to maintain scalability.

The paper is structured as follows. Section II presents the BRAIN Access Network, used in the MIND project. Section III presents the particularities of MONETs within MIND. Then Section IV introduces the proposed solutions to support MONETs within MIND. Section V makes a comparison of the three proposed solutions. Section VI concludes the paper.

II. THE BRAIN ACCESS NETWORK

The MIND project used an access network architecture developed in its predecessor project BRAIN [8]. For this reason we will refer to this Access Network as BAN (BRAIN Access Network). In BAN we have assumed an IP core network, which interfaces to the BAN through a number of BRAIN Mobile Gateways (BMG) – these act as normal IP gateways (running exterior routing protocols, firewalls and so forth). More than one BMG is recommended for resilience. At the other end of the network are BRAIN Access Routers (BARs) – IP routers with a radio link to mobile nodes – providing IP level mobility, security and QoS functions. The BAN "hides" the fact that the nodes are mobile, and all details of the particular radio access technologies, from the core. Mobile access is, at the network layer, very similar to access through DSL or UMTS (packet switched domain) at the IP backbone level. The BAN is responsible for allocating one (or more) globally addressable IP address(es) to a visiting terminal and has the basic role of delivering packets to that terminal, with acceptable QoS, as the terminal moves within the access network. This gives rise to three fundamental functions that are required within the network: mobility management, QoS and security.

User registration and AAA-related activities are controlled by a separate entity, noted by User Registry (UR). The MIND User Registration Protocol (MURP) defines in detail the process of user registration.

All network elements in the BAN are under the same administrative control. In this architecture we may identify the 'macro-mobility' as the mobility between BANs, and 'micro-mobility' within a BAN. Using concepts from existing protocols the BRAIN Candidate Mobility Protocol – BCMP was developed to specifically provide such a micro-mobility solution.

The BARs regularly broadcast their availability. When a Mobile Node (MN) receives such an advertisement and wishes to attach to the BAN through the BAR, it sends a login packet to the BAR. The BAR forwards the request to the UR, which will validate the login request. Then the UR assigns a globally routable address from a range pointing

to an Anchor Point (ANP) to the MN, and this address is sent by the BAR to the MN. This address will be changed only if the MN moves out of the reach of the current ANP. This means that the MN may handover several BARs keeping this address (micro-mobility). The BAR that the MN is attached to always keeps the MN's context with authentication and addressing information. As the MN handovers to a new BAR this context is transferred to the new BAR, *saving the need* of running the MURP again.
The data packets from a Correspondent Node (CN) outside the BAN to the MN will reach the ANP by the usual prefix based routing. The ANP tunnels received packets to the BAR the MN is attached to. In the upstream direction, the BAR reverse tunnels packets from the MN to the ANP, which decapsulates the packets and forwards them to the CN.
For more detailed information about the concepts and the architecture of the BAN, the interested reader may refer to [7, 8].

III. MONETS IN MIND

In this section we present the guidelines followed during the design of the MONET solutions in MIND. First we enlist the chief requirements towards MONETs. Then, based on possible usage scenarios, we identify several cases (we call them deployment cases) that differ in the relationship between the owners and administrators of the access domains and MONET nodes.

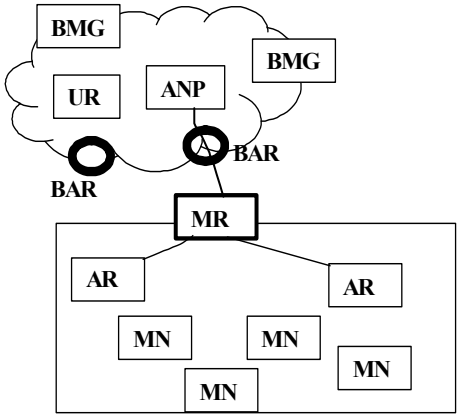

Figure 1 – Simple MONET

Our guidelines for attaching a MONET to the BAN were:
- following the BRAIN/MIND architecture,
- not modifying BCMP,
- not burdening MNs with extra functionality or protocols, additional to BRAIN
- hiding mobility, i.e., MNs within the MONET need not take any action when the MONET moves ('hands over').

We identified three MONET types that cover all the targeted MIND scenarios. Basically, the MONET in our approach (also called "Simple MONET") is depicted in Figure 1. The MONET is attached to the BAN through a Mobile Router (MR), and the MR is linked to a number of Access Routers (AR). These Access Routers provide access to the MNs of the MONET. The "Single Mobile Router" is the sub-case of the "Simple MONET", where the number of Access Routers in the MONET is limited to exactly one, and this AR is merged with the MR. Thus we confined ourselves to looking into simpler networks, which are not nested and/or multi-homed and which do not expose their "MANET-like" features. We considered that restricting the research to the above-described scenarios would let us focus on the main issues of the MONETs and will lead to well-designed protocols. It is possible that the more complicated scenarios excluded from our investigations are derivatives of these simpler ones and they may be covered by the combination of our solutions.

A. DEPLOYMENT CASES

Within the MONET scenarios, we identified three different deployment cases, as discussed below. The BAN operator may manage a MONET, or the operator of the MONET may differ from the one controlling the BAN. Furthermore, even if the BAN and the MONET belong to the same administrative domain, they might form distinct mobility management and addressing domains. We will call "tightly coupled" approach the situation when the MONET and the BAN have the same operator and they form a single mobility domain, as well. The "loosely coupled" term refers to the situation of the MONET and the BAN in a single administrative domain, but the mobility and addressing of the MONET members are handled separately. Finally, we will call the "separated domains" the case, when different operators control the BAN and the MONET. In our view, the different real-life scenarios in which the MONETs will be used justify the separation of deployment cases.

Tightly Coupled Case
The tightly coupled set-up may correspond to a small MONET, where the low number of users, thus the low gain in performance does not justify the cost of delegating some important BAN functionalities in the MR. Delegation implies a complex configuration both in MR and BAN. Moreover, the operator would not like to delegate the AAA and routing, etc., privileges to the MR, due to the widely spread (thus hardly manageable) nature of the MRs.

Loosely Coupled Case
The loosely coupled scenario typically occurs in a public transport operated network, where the transport company owns a large number of vehicles and the access hardware within. Let us suppose the case of a train operator that owns the hardware and optical fiber along the rail, as well. So this company is the operator and owner of both the BAN and MONET. It also regularly serves a large number of customers, which appear as potential MNs from the MONET point of view. In this case the trust relationship is implicitly high between the BAN operator and the

MONET. Also the larger profit and the volume of transactions make it feasible to treat this situation as a separate deployment case. Regarding the mobility management, the most important aspect of this case is that the BAN delegates the mobility and addressing responsibilities to the MONET.

Separate Domains Case
The separate domains case is a natural extension of the loosely coupled one. Not only the mobility and addressing, but also the authentication and user registration are handled separately in MONET and BAN. That means that modular and flexible deployment is possible, the internals of the MONET are independent from the BAN. This may occur at large public transport companies, which keep their own domain and relay the MNs' traffic based on roaming agreements with the BANs. Also in the case of ad hoc mobile platforms (e.g., a MANET in a train) or no regular routes (e.g., a bus hired by a company for one event only) this approach has certain advantages.
The following section details the three solutions developed to support the above-mentioned cases. All traffic between the BAN and MNs in the MONET goes via the MR. The common part of all these three approaches is that they consider the MR as logged into the BAN and further on the MR will act as a 'gate' towards the MNs. The solutions differ based on the functionalities delegated to the MR. The ISPs deploying the MONET will choose between these solutions based on their business and marketing strategies. The requirements to enable these solutions are limited to tunnelling, MANET routing, BCMP-related capabilities and/or MAC level state maintenance.

IV. PROPOSED MONET SOLUTIONS

In this section we present the three different solutions. For each solution we discuss the process of address management and packet forwarding as they are key issues in the mobility management of the MONETs.

A. PROXY MODE

As a first solution, we introduced the MR as a slightly modified MN, that has ad hoc routing capabilities, and we tried to cover the tightly coupled deployment case, when the same operator controls both the BAN and the MONET. The MR will act as a proxy between the MN and the BAN (see Figure 2)[1]. That is why we called this solution the 'proxy mode'.

Address Management
The MR has to login to the BAN through the BAR, and it will get an address from the ANP. Each MN will login to the BAN, too. The MR only conveys information, both mobility signalling and data, from the MNs to the BAR. The BCMP procedures will be executed by the BAN's elements (ANP, UR and BARs). This is the easiest solution. However, the MONET will not have a well-defined sub-network address, thus intra-MONET communication is complicated.

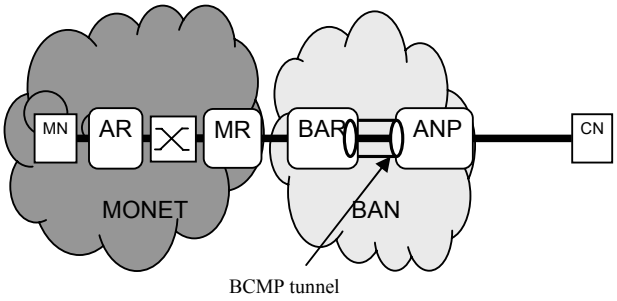

Figure 2 – MR in proxy mode

Packet Forwarding
The data packets coming from the BARs are addressed to the MNs at IP level. The MN is not directly attached to the MR, and on the route from the MR to the AR there may be other routers, as well. The router between the AR and the MR in Figure 2 depicts this situation. Thus the packet is routed through the MR and (possibly) other routers from the MONET to the MN. The routes are maintained by the routing protocol run in the MONET. The upstream packets (from MN to BAR) are routed by the network elements (AR, intermediate routers, MR) in the MONET. The BAR-to-ANP tunnel in Figure 2 is the BCMP tunnel assuring the packet forwarding between the BAR and ANP.

B. PREFIX MODE

Complementary to the proxy mode, the BAR may delegate some of its functionalities to the MR in order to simplify the MN-to-BAN signalling (Figure 3). This also requires a trust relationship between the BAN and the MR. This relationship is implicitly established if we suppose that the same operator administers the BAN and the MR (loosely-coupled deployment case). Otherwise (separate domains case) the AR to BAN communication is based on the MR's agreement with the BAN.

Address Management
We consider that in this scenario the MR controls the MONET as a subnet delimited by its own address and a prefix. Therefore we called this solution the prefix mode. The MR has to login to the BAN through the BAR, and it will get an address from the ANP. The MR should obtain the prefix defining the subnet from the ANP, as well. Now each MN will login to the ARs in the MONET and not the BARs on the ground. This implies that the MRs should implement some UR and ANP functionalities so that it can assign MNs addresses from its prefix. This is the reason Figure 3 includes the "ANP" tag in the MR. Also the ARs may have similar responsibilities as the BARs. In this case the ARs will store the context of MNs and the MNs have

[1] In the figures we show a single network element that implements both UR and ANP functions, denoted "ANP".

to perform a handover if they move from one AR to another. The BCMP tunnel within the MONET refers to this situation.

Packet Forwarding
Each downstream packet is tunnelled via the BCMP tunnel from the ANP to the BAR, and then the BAR will forward it to the MR, based on the prefix of the MONET. The MR will route the packet inside the MONET to the MN. The MR uses the BCMP tunnel between the MR and the AR, if BCMP is used in the MONET (see the BCMP tunnel in the MONET in Figure 3). The packets from the MN are sent to the AR, then tunnelled to the MR. The MR, based on the prefix, realises that the packet is destined to a different subnetwork, so it routes to its default gateway, the BAR.

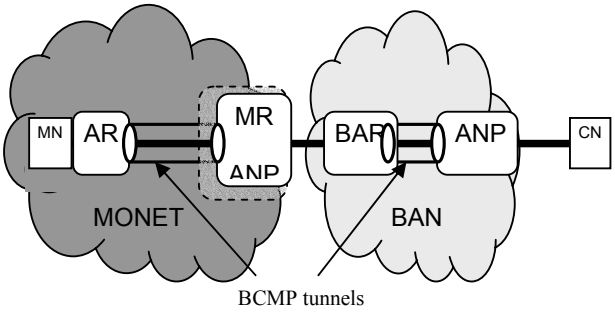

Figure 3 – MR in prefix mode

C. ENCAPSULATING MODE

In this scenario we nest the original BAN into another BAN (see Figure 4). This latter BAN will provide a BCMP service to the MNs of the MONET. Since the BAN supporting the MR (the original one) is different from the BAN supporting the MNs, the encapsulating mode corresponds to the separate domains case.

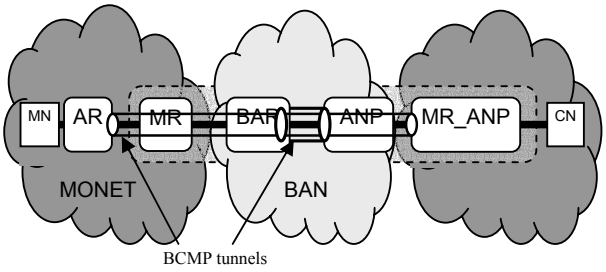

Figure 4 – MR in encapsulating mode

Address Management
When the MR moves into the coverage area, it logs in to the BAN. It will get an address from the ANP and registers with its MR_ANP. The MNs will login to the ARs, and the ARs will act as BARs. The addresses assigned to the MNs are delivered from the MR_ANP's address space.

Packet Forwarding
The BAN will handle all the traffic from the MR as usual client traffic. The particularity of this traffic is that it is always destined to the same Correspondent Node, namely the MR_ANP. All traffic, including the login messages, coming from the MN traverses the AR-MR-BAR-ANP-MR_ANP path. Then the MR_ANP will distribute the packets to the CNs originally addressed by the MNs. We will have a MR-to-MR_ANP tunnel, which is further tunnelled over the BAR-ANP segment. The first tunnel is handled by the MONET's BCMP, the second one by the BAN's.

V. COMPARISION

Each of the three MONET solutions have certain advantages and drawbacks. In this section we try to highlight these characteristics. We consider that the decision of deploying one of these solutions is not a pure engineering one, since it is greatly influenced by the business environment of the service provider.

Proxy Mode
The MNs will have the freedom to negotiate their services directly with the BAN, thus enhanced service personalisation is enabled. However, at each BAR-handover, the MNs have to update their default gateway addresses.
We specified some add-on functionalities to the BAR architecture that automatically transfers the MNs' context as the MONET moves from one BAR to the other. We called this solution the Automated Context Transfer [3]. This solution has the advantage of relieving the MR-BAR interface from the signalling load at handovers. This solution also requires configuring the MR as a proxy that will distribute the address of the new BAR within the MONET.

Prefix Mode
In this solution, at BAR handovers the MNs do not have to receive any information regarding the new BAR. Since the upstream traffic is routed based on the prefix, it is enough that each MN configures the MR's or AR's address as the gateway.

Encapsulating Mode
The result of this method is that it completely hides the MR's mobility from the MNs. On the other hand, all the MNs are linked to the MONET. That means they must logoff from the MONET as they move out from the coverage area. This implies that a MN's address changes as the user gets on or off from the train.

Modes	Advantages	Disadvantages
Proxy	*simple deployment*	*greater burden on ANP*
Prefix	*compact solution*	*ANP changes are not hidden completely*
Encapsulating	*completely hidden mobility*	*Longer routes because of anchoring at MR ANP*

Table 1. Comparison of the solutions

We highlight in Table 1 the major advantages and disadvantages of each solution. An operator might choose the proxy mode to introduce the service as a quick upgrade to an existing system. The prefix mode requires more effort, since it may involve the software upgrade in access network elements, but it offers better performance. The encapsulating mode fits the needs of those operators that want to separate their service from the one offered by the access networks.

The features of the three proposed solutions are compared on a qualitative basis. We consider that a quantitative comparison should primarily focus on the signalling load and the handover delays induced by each solution. Therefore we direct our future research efforts towards a quantitative analysis on these issues.

VI. CONCLUSIONS

The fundamental goal of mobility management is to deliver packets to a mobile end-system. MIND presents significant challenges beyond those faced in the BRAIN network architecture, primarily because the concept of individual mobile hosts connecting in a single hop to a homogenous access network is no longer valid. A starting assumption was that the BRAIN Candidate Mobility Protocol (BCMP) should be re-used where possible. The major improvement required in BCMP is the need to allocate address prefixes, not just single addresses. We tried to minimise the signalling load and avoid burdening MNs with extra functionality, additional to BRAIN protocols.

For the moving network (MONET) three possible solutions were proposed: proxy, prefix and encapsulating modes. Which one an operator selects depends largely on the commercial details of the given MONET scenario and particularly on whether the BAN and MONET operators are the same, devolved, or independent.

ACKNOWLEDGMENTS

This work has been performed in the framework of the IST project IST-2000-28584 MIND, which is partly funded by the contributions of their colleagues from Siemens AG, British Telecommunications PLC, Agora Systems S.A., Ericsson AB, France Telecom S.A., King's College London, Nokia Corporation, NTT DoCoMo Inc, Sony International (Europe) GmbH, T-Systems Nova GmbH, University of Madrid and Infineon Technologies AG.

REFERENCES

[1] IETF NEMO- NEtwork MObility Working Group, http://www.ietf.org/html.charters/nemo-charter.html

[2] Charles Perkins, "IP Mobility Support", IETF RFC 2002, October 1996.

[3] MIND Deliverable 2.2, "MIND protocols and mechanisms specification, simulation and validation", from www.ist-mind.org, 2002.

[4] IST 1999-12515 project DRiVE- Dynamic Radio for IP-Services in Vehicular Environments, http://www.ist-drive.org, 2000.

[5] IST 2001-35125 project OverDRiVE- Spectrum Efficient Uni- and Multicast Services over Dynamic Multi-Radio Networks in Vehicular Environments, http://www.ist-overdrive.org, 2002.

[6] David Johnson, Charles Perkins, "Mobility Support in IPv6", draft-ietf-mobileip-ipv6-18, Work in progress, 1 June 2002.

[7] IST 2000-28584 Project MIND- Mobile IP-based Network Developments, http://www.ist-mind.org, 2000.

[8] IST 1999-10054 Project BRAIN- Broadband Radio Access for IP-based Networks, http://www.ist-brain.org, 1999.