Interoperable Networks for Secure Communications

Task 3 (Mobility) Final Report

14 July 2006

This report documents the results and conclusions from Task 3 (Mobility) of the INSC Program, Phase 2.

This report was developed with contribution from the following task members.

Joseph Macker	T3 TL
Jeff Weston	US POTL (Editor)
Louise Lamont	CA POTL
Thierry Plesse	FR POTL
Harald Bongartz	GE (FGAN) POTL
Wolfgang Fritsche	GE (IABG) POTL
Ivano Guardini	IT POTL
Boris Kock	NL POTL
Knut Øvsthus	NO POTL
Michael Clarke	UK POTL

Table of Contents

Executive Summary i
1 Introduction 1
2 Dynamic Wireless Routing Technology 1
2.1 MANET Testing Framework 2
2.2 MANET Unicast Work 6
2.3 Simplified Multicast Forwarding Work 13
2.4 Other MANET Multicast Protocols 18
2.5 Multicast Protocol Comparison 19
2.6 Multicast Gateway Functionality 24
2.7 Black-Side MANET 27
2.8 MANET Autoconfiguration Work 27
3 Edge Mobility Technology 34
3.1 Mobile IPv6 Autoconfiguration 35
3.2 NEMO Technology 41
3.3 NEMO Testing Framework 42
3.4 Linux NEMO Functionality Testing 50
3.5 NEMO Performance Testing 53
3.6 NEMO Conclusions 61
4 Hybrid MANET-Edge System Mobility 62
4.1 MANET-MIPv6 62
4.2 MANET-NEMO 72
5 Exploitation and Transition 73
5.1 IETF Transitions 73
5.2 Related Field Tests and Experiments 74
6 Conclusions 79
6.1 Dynamic, Wireless Routing 79
6.2 Edge Mobility 80
6.3 Other Technologies 81
7 Operational and Future Work Recommendations 81
7.1 Dynamic, Wireless Routing 81
7.2 Edge Mobility 82
7.3 Other 83
ANNEX A: RELATED ACTIVITIES 84
ANNEX B: GLOSSARY 88
ANNEX C: REFERENCES 92

Executive Summary

The INSC Mobility Task Area, Task 3 (T3), was responsible for investigating technical solutions that support improved network mobility within a future coalition network architecture. Additional T3 technical goals included examining evolving open standard Internet Protocol (IP) based solutions to better support interoperability and heterogeneity, investigating both IPv4 and IPv6 mobility enhancements, and analyzing technical issues relating to military adaptation of evolving open standard protocols. T3 focused its main efforts on the examination of related open standard network protocols and not on the particular wireless technologies that these protocols may eventually run on top of. This executive summary provides a brief overview of the various mobility technologies investigated by Task 3 and summarizes results and recommendations from our coalition experimentation. For additional background on technology issues, please refer to additional documentation contained in the Task 3 Mobile Networking Technology Assessment and Considerations Document [1].

Mobile Ad hoc Network (MANET) Research and Demonstration Efforts

In carrying out this joint coalition research effort, there were two main network protocol work areas that INSC Task 3 focused on: dynamic, wireless routing technology (e.g. MANET) and edge system mobility technology (e.g. MIPv6, NEMO). To supplement other INSC Task work demonstrated in more traditional fixed local area networks, the INSC II T&D Architecture included multi-hop, mobile ad hoc network (MANET) routing areas at the edges to represent “last tactical mile” wireless network scenarios. A capability demonstration of MANET providing a mobile routing region within the secure backbone routing domain was also done. In addition to field testing and simulation tools, INSC integrated a distributed set of mobile network emulation testbeds at the edges of the testing infrastructure to enable controlled and repeatable testing of mobile networking technology and alternative protocol techniques. Variations of the Optimized Link State Routing (OLSR), MANET Extensions to OSPF (MANET-OSPF), and Ad hoc On-demand Distance Vector (AODV) protocols, worked on within the Internet Engineering Task Force (IETF), the primary Internet Standards body, were the main set of MANET unicast routing protocol applied within join coalition testing. Variations of the protocols and protocol parameters were tested under various conditions by different participating organizations (POs). End-to-end functional testing was also performed between coalition partner facilities and laboratories operating separate MANET routing areas. The MANET routing testing and demonstrations within INSC II concentrated mainly on newer IPv6 capabilities, but IPv4 capabilities were also demonstrated and supported. The INSC II MANET testbed supported both IPv4 and IPv6 capable end systems and enabled end-to-end testing of a variety of applications (e.g. mail, chat, web, p2p, video, VoIP) and specialized test traffic tools.

The Simplified Multicast Forwarding (SMF) MANET multicast protocol, now being progressed within the IETF MANET WG as a candidate specification, was used in INSC II by a variety of POs to demonstrate mobile multicast data forwarding within highly dynamic MANET routing areas. Since present off-the-shelf multicast routing standards were not well-suited for MANET environments, this new MANET-enhanced multicast

routing protocol was targeted for demonstration in addition to the testing and demonstration of MANET unicast routing. A variety of optimized relay set algorithms were tested and also demonstrated within SMF. SMF supported the demonstration of multicast test traffic, streaming video, VoIP, multicast chat, situational awareness, and other applications within the INSC II demonstration laboratories.

Edge Mobility Research and Demonstration Efforts

As mentioned, INSC II T3 also examined edge system mobility technology. With this technology, the INSC II T&D Architecture supported roaming mobile nodes and whole subnetworks within the secure wide area network (WAN) infrastructure while allowing nodes and networks to maintain assigned network address spaces. The primary single host based technology targeted for test and demonstration to support this was MobileIPv6. As in Phase I, surrogate roaming agents and home address assignments were used to emulate the mobility of nodes throughout the architecture. End-to-end communications functionality and performance were tested and demonstrated during mobility scenarios. In addition to roaming mobile nodes across the secure WAN as done in Phase I, the INSC II T&D architecture tested and demonstrated the roaming of aggregate networks across the WAN through the use of such IETF technologies as Network Mobility (NEMO). This technology may be suitable for aggregate platform networks that move “as a whole” and require support of seamless macro mobility across a broad possibility of network attachment points. INSC II developed candidate scenarios to demonstrate the application of aggregate network mobility and end-to-end interoperability. This technology is not an alternative to MANET routing but potentially solves a different form of network mobility problem.

Other Technology Research Efforts

Task 3 also demonstrated significant advancements in both MIPv6 and NEMO operation by examining the potential for integration within an operation MANET network. Additionally, there are some technologies investigated which had an impact in both MANET and edge mobility. Cross layering is becoming more mature, and several science and technology projects, including INSC, have begun to demonstrate the value of such design approaches. INSC Phase II examined newer advancements in autoconfiguration for both MANET and edge mobility. The ability to autoconfigure MANET using stateless autoconfiguration was demonstrated, as was Home Agent autoconfiguration for MIPv6/NEMO.

Summary of Mobile Network Technical Observations

Dynamic, Wireless Routing

Mobile Ad hoc Network (MANET) technology is useful for supporting military network regions requiring self-organization, mesh operation, and possible high mobility. Since Phase I of INSC, advancements have occurred in both performance extensions and IPv6 support within basic unicast MANET routing. Some existing MANET unicast routing protocols are relatively mature including the Optimized Link State Routing (OLSR) Protocol and the Ad-hoc On Demand Distance Vector (AODV) Protocol, but

newer designs continue to evolve within the IETF (e.g., MANET-OSPF, OLSRv2, DYMO). These MANET protocols support both IPv4 and IPv6 operations.

Different MANET protocols have different performance behaviors, and while a subset of 2 or 3 may cover most military scenarios, there is no “one size fits all” design at present. The appropriateness of different solutions has been shown to be related to the intended operational scenarios, applications, and platform requirements (e.g., proactive vs. reactive, vehicular vs. manpack, convoy vs. cluster at deployed HQ, local vs. non-local communications). Additionally, within INSC some MANET implementations and concepts were discovered to be more mature than others.

Newer MANET multicast routing was examined within INSC Phase II and work is now evolving within the standards community as well. Simplified Multicast Forwarding (SMF) is a prime example of an approach that can support improved group communication operations in localized highly mobile routing areas. INSC Phase II demonstrated the use of various test traffic and applications over SMF including: streaming video, VoIP, mobile multicast chat, file transfer. This technology is also supporting improvement in MANET and mobile technology autoconfiguration techniques. Several connected dominating set (CDS) algorithms for flooding overhead reduction were investigated by T3 within SMF, providing a range of solutions with differing levels of overhead, distributed operation, and mobility robustness. In addition to SMF, group based multicast (e.g. MOLSR, MFP) was also examined as an alternate MANET multicasting strategy. With these protocols, multicast transmissions are confined to only those nodes on the forwarding path of the multicast group subscribers (which may change over time). This may reduce the amount of loading placed on the network compared to optimized flooding in certain topologies when the number of subscribers is much smaller than the total number of optimized relay set nodes in the network. However, it is unclear how much performance may be gained, given the added complexity of maintaining subscriber and forwarding trees under mobility for each multicast group in the network.

MANET autoconfiguration has also been an important work item within INSC Phase II and the results will be of value to the operational community in order to both reduce the time needed to deploy their tactical networks and reduce the amount of skilled pre-configuration these networks would otherwise require. Stateful (DHCP) and stateless (distributed router advertisements) methods for IP address and default gateway autoconfiguration were investigated. In addition, a distributed DNS system known as DMDNS was designed and tested within INSC to overcome mobility issues faced by standard DNS within MANETs.

Edge Mobility

Mobile IPv6 and potential extensions (hierarchical MIP) were investigated by Task 3. MIPv6 implementations have become more mature and have become more widely available, but the inclusion of IPSec integration into the protocols is still evolving. Standard specifications for Hierarchical MIP have advanced more slowly than

anticipated at the beginning of INSC Phase II and have been studied less during this time period.

Network Mobility (NEMO) provides newer technology enhancement for aggregate prefix mobility. As a newer technology extension of MIPv6 concepts, NEMO may provide more relevant military support for larger platform and network mobility across and within WAN architectures. Task 3 investigated this technology's basic modes and some extended operational modes (e.g., NEMO nesting). Basic NEMO is presently functional, but implementations are still not stable (more testing is recommended). At present, software bugs and missing protocol features have been discovered by Task 3 researchers. The NEMO nesting function (multiple NEMO tunnels) has been shown to work, but there is little experience with the performance impact of current solutions. There are also important architectural issues resulting from additional encapsulation with each nesting level.

There may be architectural and scenario-specific issues related to the use and distribution of home agent functionality. For instance, in a tactical scenario, the home network provides a single point of failure. Further investigation is needed in this area. Additionally, tests performed by Task 3 showed that current protocols may not be sufficient for fast handoff latency scenarios without additional engineering attention. Finally, INSC Phase II also demonstrated the ability to autoconfigure the MIPv6/NEMO Home Agents.

Other Technologies

Task 3 also demonstrated significant advancements in both MIPv6 and NEMO operation by examining the potential for integration within an operation MANET network.

Additionally, there are some technologies investigated which had an impact in both MANET and edge mobility. Cross layering is becoming more mature, and several science and technology projects, including INSC, have begun to demonstrate the value of such design approaches.

Summary of Mobile Networking Recommendations

Dynamic, Wireless Routing

Task3 recommends that MANET solutions be considered for tactical edge routing scenarios and that prior to any deployment additional technical efforts should address design integration with evolving tactical wireless technologies. Each wireless technology and MAC layer will present different opportunities, challenges, and performance issues. INSC has studied a variety of MANET unicast routing solutions evolving within the Internet open standards community. Proactive MANET routing approaches, such as OLSR and MANET-OSPF, are recommended for consideration when more constant communication support is needed and robustness is desired, especially intra-vehicular. The overhead for these protocols can be better engineered and is more predictable under a variety of traffic and mobility conditions. Reactive protocols, such as AODV or DYMO, may be useful when energy constraints are a

paramount concern and traffic flows are sparse (e.g., sensor networks). All MANET approaches studied support localized routing under node mobility in addition to the ability to advertise prefixes or additional subnetworks attached to a node (e.g., vehicular LANs, etc).

T3 recommends that optimized wireless multicast forwarding solutions, such as Simplified Multicast Forwarding (SMF), be integrated into future tactical edge network systems. SMF can provide efficient delivery of application data within a MANET routing area. This can provide increased efficiency for a variety of applications (e.g., situational awareness, multicast VoIP, video streaming, chat, etc). T3 demonstrated a variety of multicast IP application working within prototype mobile networks using SMF. T3 also recommends that further work be done in the area of group-based multicast to investigate the robustness of such protocols and determine whether significant performance gains can be made compared to flooding techniques such as SMF.

T3 recommends that MANET solutions initially be considered for stub network deployments to support the tactical edge. Future transit network applications and more complex gateway interactions can be supported, but would require more study concerning the scalability of current approaches and considering scenario specific requirements. MANETs should also be planned for deployment with consideration for appropriate hierarchies, multiple MANET routing areas rather than larger flat routing areas.

Further work on MANET autoconfiguration is recommended and early work by T3 shows promise in the areas of MANET/edge integration and the use of SMF for supporting autoconfiguration and discovery services. Competing techniques should be compared and recommended for specific operational scenarios. This work should contribute to the emerging IETF MANET autoconfiguration WG standardization efforts in order to achieve widespread acceptance and vendor compatibility in future Coalition operations. Further development of DMDNS is recommended to resolve the outstanding technical issue of interfacing with standard DNS and to fully assess its scaling qualities.

If MANET devices are deployed primarily as routers, they may be configured to use unnumbered or link local addresses (IPv6) to ease the burden of configuration. In this case, the MANET routers would serve to support and advertise attached prefix addresses and would operate similar to fixed infrastructure IP routing configurations. One issue here is that it is recommended that unique MAC or 64 bit IEEE EUIDs be deployed so that complex duplicate address detection (DAD) schemes can be avoided.

Edge Mobility

Edge Mobility Technology enhancements (e.g., NEMO and MIPv6) provide benefit in some example tactical use case scenarios developed by T3. If devices or platforms are required to maintain their global IP addresses or prefixes when mobile across an infrastructure, then NEMO and MIPv6 can provide benefits. NEMO provides additional benefits when blocks of addresses are expected to move as whole networks (e.g.,

ships, vehicular LANs, etc). If low-latency connection handoff scenarios are important, edge mobility solutions need additional engineering attention prior to deployment consideration. MIPv6 and NEMO can directly support the retention of active network connections since the endpoint addressing does not change. Further studies are recommended to be conducted to examine application and transport specific performance in this area.

NEMO handles aggregate network prefixes mobility (platform mobility scenarios). This is useful for various use cases given mobility within a larger military backbone network and we recommend this be considered as a possible solution for those cases. This may have a side benefit of improving overall network management since home addresses can remain static. If mobility is expected to be largely localized within a topology a routing protocol or MANET solution may be a better choice. Since we expect both localized and macromobility situations to occur, we recommend both technologies be considered for deployment.

Other Issues

It should be noted that while T3's work was done mainly at Layer 3 (IP), the technologies and algorithms can also be applied at Layer 2 if desired. Layer 3 has a heterogeneous and cost value since it is somewhat technology-agnostic. It is also possible to combine the two solution types. T3 recommends more consideration be given to cross layer performance to improve efficiency performance and delay. One example is the use of lower layer interface information to improve neighbor link status, activation, and deactivation.

T3 recommends that future work address issues in supporting specific scenarios and examine particular protocol extensions and optimizations as appropriate to support architectural and mission needs (e.g., EMCON nodes). We also recommend further attention be paid to security requirements in future work. At present, we recommend that particular security solutions are scenario dependent.

1 Introduction

The Interoperable Networks for Secure Communications (INSC) project is an international collaborative research and development activity between Canada, France, Germany, Italy, Norway, the Netherlands, the United Kingdom and the United States, with invited contributions from the NATO Consultation, Command and Control (C3) Agency. The objective of the project is to specify, implement, test, and demonstrate a common technical architecture for interoperable secure networks with mobility extensions, using commercial technologies, products and solutions wherever possible. The INSC Phase II project is broken down into subtask elements. The Mobility Task, Task 3 (T3), was responsible for investigating solutions that support improved network mobility within a future coalition network architecture. Additional T3 technical goals included examining evolving IP-based solutions to better support interoperability and heterogeneity, investigating both IPv4 and IPv6 mobility enhancements, and analyzing technical issues relating to military adaptation.

There are two main technical work areas that T3 focused on: dynamic, wireless routing technology (e.g. MANET) and edge system mobility technology (e.g. MIPv6, NEMO). This report gives a brief overview of the various mobility technologies investigated by Task 3, and documents the results from our experimentation. Lessons learned and recommendations for future research are also detailed within this report. More detailed descriptions of these mobile networking technologies and guidance on where they should be considered for operational deployment, along with some information on the benefits and issues associated with each of the technologies, can be found in the *T3 Mobile Networking Technology Assessments and Considerations* document [1]. Additionally, a summary of the work done by the Mobility Task in INSC Phase I can be found in the *Task 6 Final Report* [2].

2 Dynamic Wireless Routing Technology

Dynamic wireless routing is generally a more localized, or intra-domain routing, type of mobility solution. This type of technical solution is applicable to a wide range of military tactical network scenarios involving wireless technology and unpredictable or changing topological arrangements amongst nodes. INSC Phase II examined IP routing protocol functionality suitable for wireless routing application within both static and dynamic topologies. While IP routing protocols commonly in use on the Internet today (e.g. RIP [3], OSPF [4] [5], BGP [6], etc.) are designed to handle network changes, they are not designed to cope with the high rates of change and unreliable channels inherent in mobile wireless networks. They are also generally designed with the assumption that data coming in an interface should never be forwarded back out that interface, which is a valid assumption for the standard wired infrastructure routers in use on the Internet, but is not valid with typical broadcast packet radio interfaces. Although a broad range of academic work and dynamic wireless routing technologies are available, Task 3 focused on the area of Mobile Ad Hoc Networking (MANET) evolving within the Internet Engineering Task Force (IETF). The fundamental MANET problem areas being addressed are that wireless link interfaces have some unique routing interface

characteristics and that node topologies within a wireless routing region may experience increased dynamics, due to motion or other factors. Evolving IETF MANET specifications fundamentally provide improved operational IP routing performance for dynamic, wireless routing regions. Approaches are intended to be relatively lightweight in nature and suitable for heterogeneous adaptation across multiple hardware and wireless environments and for adaptation to small, embedded systems where needed.

While MANET routing areas may operate in isolation from a larger connected Internet, a primary focus of the INSC II Task 3 work is to address its use as a routing technology extension at the edges of a coalition network. The technology directly supports a greater dispersion of forces and resources, allowing network connections to beyond line-of-sight (LOS) or beyond the capabilities of a single radio asset. The deployment of hybrid mesh infrastructures (e.g., a mixture of preferred fixed or resource advantaged nodes and highly mobile, disadvantaged routers) can also be supported by MANET specifications and management approaches and such a capability is considered important for tactical environments. In this way, without sacrificing flexibility-advantaged platforms or key network relays, nodes can be placed and preferred within the architecture when possible. The self-organizing nature of this technology makes it suitable for use in disaster relief (no infrastructure) or obstructed wireless environments (e.g., within manmade or natural structures).

2.1 MANET Testing Framework

There are a variety of unicast and multicast routing protocols for MANET. The main MANET routing protocols investigated by Task 3 members were Optimized Link State Routing (OLSR) [7], Ad Hoc On-Demand Distance Vector routing (AODV) [8], and MANET-OSPF [9] for unicast and Simplified Multicast Forwarding (SMF) [10] for multicast. Each of these protocols has different behavioral characteristics. For instance, OLSR and MANET-OSPF are proactive routing protocols, meaning that they always maintain routes to every other node in the network, while AODV, a reactive protocol, only finds and maintains routes as they are needed. Each protocol also has various parameters that can be modified to improve movement detection and various aspects of performance, often at the expense of additional protocol overhead. Perhaps more importantly, the effectiveness of each protocol varies as a result of the scenario in which they operate. As a result of this, a variety of network topologies, network performance parameters, traffic patterns and motion models must also be taken into account when evaluating the relative merits of each protocol.

Individual POs conducted many localized experiments to understand the functional and performance characteristics of the chosen protocols by varying network topologies, mobility models, traffic scenarios, number of nodes, and the values of various protocol parameters.

Example studied network topologies include:

- *Line*: representing a convoy of platforms or the ‘stringing out’ of communications resources to achieve the maximum coverage range.

- *Tree*: representing the hierarchical dispersal of forces with a root at the top of the local chain of command and leaves representing the lowest echelons.
- *Cluster*: could represent a Headquarters (HQ) consisting of a number of nodes interconnected by a backbone network.
- *Mesh*: this is the most general case of military organization that could occur at any time during a tactical operation and could be sparsely or densely connected in terms of radio connectivity between nodes at different times.

Tactical mobility models applicable to these base network topologies include:

- The movement of one or more nodes alongside a fixed convoy.
- The swapping of positions between individual leaves and trunk nodes and attached leaves in the tree network, representing tactical redeployment.
- The purposeful movement of HQs by changing their point of attachment on the backbone of a cluster network, thus representing the redeployment of that HQ.
- The random or random vector motion model is particularly applicable to the mesh network topology and models more random motion at various speeds within a fixed space, thus varying the connectivity between the nodes depending on the radio range and other factors. This type of mobility can often lead to temporarily or long term fragmented networks and this physical behavior may skew the evaluation of protocol performance. However, it is important that fragmentation and coalescing of localized MANET routing be supported and function effectively.

The network traffic profile is an important factor in analyzing protocol performance. Examples of traffic profile attributes include:

- *Distribution of senders and receivers*: this follows from the requirements of the application(s) being used. Some traffic distribution models include:
  - One-to-One, e.g. a file transfer
  - One-to-Many or One-to-Multicast, e.g. command instructions
  - Many-to-One, e.g. status reports to HQ
  - Many-to-Many or Many-to-Multicast, e.g. situational awareness, VoIP
- *Amount of traffic*: represents an overall loading on the capacity of the network by one or more nodes sending and forwarding traffic. If the limit of the network capacity is approached, then the amount of traffic being received by the receiver(s) will diminish due to a number of factors such as queue overflows and wireless contention and collision events. Protocol performance under congestion conditions may be more critical to military scenarios, and this may favor proactive protocols that have better performance under congestion, but may exhibit higher overhead during light loading. On the other hand, some networks may favor more reactive approaches or optimizations to proactive protocols to maximize battery lifetimes for disadvantaged nodes.

- *Type of traffic*: the traffic offered to the network by each sending node may be periodic (e.g. a video stream), or bursty (e.g. web traffic). Additionally, the interval between traffic activities can also be significant, as long intervals of inactivity could affect the performance of a reactive protocol.

Each routing protocol has its own parameters that can be adjusted to change performance characteristics, but there are common parameters that are applicable to most protocols. Efforts were made to ensure that these common parameters were as identical as possible when direct protocol comparisons were being made. However, for non-common parameters, the default values were often used. For example, most protocols have Hello packets which are sent periodically and are used to detect neighbors. Most protocols also have a related timeout value which controls when a link should no longer be considered valid because no timeout has been received. Most protocol parameters have some sort of tradeoff associated with them. For instance, significant OLSR parameters include the Hello interval, TC interval, Hello timeout and TC timeout. All of these parameters trade the responsiveness of the protocol to topology changes against the overhead required to detect and react to the change. In addition, any neighbor sensing hysteresis control values are useful in avoiding flip-flopping of link availability perception due to multipath, fading, or packet loss that can occur with wireless communications. The value and usefulness of hysteresis is dependent upon the real world wireless and mission environments. The use of hysteresis can improve stability of link sensing, but adds a penalty of additional sensing delay. During testing, some protocols were compared which did not provide hysteresis, and it is important to remember that these results may vary as environmental and testing conditions change. This is an important lesson learned and T3 has documented that enhanced interfacing between the IP routing layer and lower layer link sensing function may improve detection performance dramatically, and avoid much of the overhead due to link detection mechanisms.

Depending on the purpose of each experiment, data was collected, logged and analyzed based on a number of metrics of interest:

- *Throughput* measures the amount of user traffic being delivered on the network to one node or all nodes at a given time. This is an instantaneous measure of the rate that traffic is being delivered across the network and should approach the capacity of the network under congestion.
- *Goodput* measures the amount of useful user data being delivered to one or all nodes at a given time. It is different than throughput because it does not include duplicate or forwarded packets. Goodput can be a more difficult metric to measure with standard network layer tools than throughput, but is of more relevance to the user. T3 has used tools such as the MGEN and TRPR, developed by NRL, to measure goodput and many other statistics throughout T3 mobile network experiments.
- *Total network loading* represents the total amount of traffic (both user- and routing protocol-generated, including duplicate and forwarded packets) being

transferred across a network at any given time. Under congestion, this should be roughly the capacity of the network.

- *Routing protocol overhead* measures the amount of network traffic produced directly by the routing protocol as part of its normal operation (e.g. hello and control packets). The higher this value, the less network capacity is available for user traffic. Typically, increased routing overheads are used to provide some advantage elsewhere, such as increased responsiveness to topology events.
- *Latency* measures the time it takes for a transmitted packet to traverse and arrive at the destination network node(s) from the original source node. Some real-time applications (e.g. VoIP) require some average bounds on latency to be useful. These bounds may be longer in tactical networks than in traditional fixed infrastructure telecommunication networks.
- *Initial route discovery time* is one significant measure of the tradeoff of routing overhead between reactive and proactive MANET protocols. Because proactive protocols maintain all routes across the network at all times, they are able to more quickly support new traffic flows entering the network for previously unused destinations. In contrast, reactive protocols must establish a route for particular destinations before routing the first user packet in a flow, creating a higher initial latency in packet delivery or possible causing some packet loss for real time data.
- The percentage of *packet loss* during a mobile network scenario is also a metric Task 3 measured in some cases.

Although often conducted by various POs, MANET experimental analysis has been peer reviewed at T3 meetings in order to reach some group consensus on the methods and conclusions of the analysis. Some of this work is reported in detail in separate INSC whitepapers with important results and conclusions that are summarized later in this document.

Most T3 POs continued to use 802.11-based Wireless LAN technology as a proof-of-concept wireless ad hoc link in simulated, emulated, and live test configurations. A number of PO sponsors are considering the deployment of 802.11-variant technologies as part of a requirement for mobile communications. Some POs also used other wireless technologies (e.g. Bluetooth), but very little detailed or scaled testing was done with other wireless technologies due to budget and time constraints. The Medium Access Control (MAC) layer used by 802.11b is a contention based access scheme known as Carrier Sensed Medium Access Collision Avoidance (CSMA/CA). With this scheme, it is still possible for multiple nodes in a network to simultaneously transmit on the shared medium thus causing a collision and loss of data at a shared receiver. This possibility increases as the loading in the network increases. For unicast data, contention mitigation strategies (RTS/CTS) can improve multiple access statistics. 802.11b supports a range of link bandwidths up to 11Mbps. A commonly used default chosen by many POs was 2Mbps as this was high enough to support bandwidth intensive applications such as video, while also demonstrating good link stability.

Emulation and simulation methods and systems were used by Task 3 in the investigation of MANET protocols. Several emulation platforms were made available to the Task by T3 POs. NRL's Mobile Network Emulator (MNE) [11] uses *iptables* to block IP packets by MAC address, and supports emulation using real wireless LAN cards. The UK's Large Network Emulator (LNE) makes use of a managed switch to maintain Virtual LANs (VLANs) for groups of nodes which can hear one another. While emulation is not a replacement for live field testing or simulation, it can be used to test real implementations of MANET protocols using real hardware, without incurring the high expense associated with live field testing. Simulation is also useful for investigating how MANET protocols scale up to large numbers of nodes. In many cases, the MANET prototype software used in emulation (e.g. NRLOLSR [12]) was also supported and used within simulation environments such as ns2 [13] and OPNET [14] and within real world experiments.

Dynamic, wireless routing technology such as MANET is best suited to support localized types of mobility that can be managed by an intra-domain routing solution. Therefore, most T3 MANET testing was done in a localized fashion, without making use of the INSC WAN. The WAN also had much lower capacity than the localized mobile wireless network links T3 was working with and would dramatically affect end-to-end results. However, MANET-to-MANET PO WAN testing was done for most MANET protocols in order to demonstrate their gateway and application support capabilities, often in a static fashion by envisioning the MANET as a stub network with a common, unique prefix.

2.2 MANET Unicast Work

The MANET unicast protocols examined in some detail by T3 include Ad Hoc On-Demand Distance Vector routing (AODV), Optimized Link State Routing (OLSR) and some functional variants, and MANET extensions to Open Shortest Path First (MANET-OSPF). These three protocols provide a good representation of open standards work in MANET routing evolving within the IETF community. Additional work was done by some POs on some nonstandard protocols.

In addition to performance testing with MGEN [15], various real applications were also functionally tested over these MANET protocols. Voice-over-IP (VoIP), video streaming, web browsing, and chat applications have all been run over these networks successfully.

2.2.1 Optimized Link State Routing (OLSR)

Although significant Optimized Link State Routing Protocol (OLSR) MANET protocol evaluation and testing was done in Phase I of INSC, more advanced work and examination of newer protocol features has continued in Phase II. OLSR has been documented as IETF Experimental RFC 3262 [7]. In addition, a newer standards track specification effort has begun within the IETF to specify OLSR version 2 (OLSRv2) [16]. Fundamentally, OLSR operates as a table driven and proactive protocol, exchanging topology information with other nodes of the network regularly. Several

implementations of OLSR prototype code were used within INSC Phase II. These include:

- NRLOLSR developed by NRL (US) [12]
- CRCOLSR developed by CRC (CA) [17]
- Unik OLSR developed by Unik, Norway [18]
- OLSR developed by INRIA [19]

Newer technology advancements with OLSR that have been tested since Phase include additional IPv6 enhancements, full vs. partial topology modes (NRLOLSR), the use of plug-ins (Unik), multiple platform support (including PDAs, embedded computers, and simulators), and some signal quality enhancements.

To optimize flooding and reduce protocol overhead, OLSR uses the concept of multipoint relays (MPRs). Nodes which are selected as an MPR by one or more neighbor nodes announce this information periodically in their control messages. In route calculation for partial topology, the MPRs are used to form potential routes from a given node to any destination in the network. The protocol uses the concept of MPRs to facilitate efficient flooding of control messages in the network and to reduce the size of topology announcements by only announcing a partial topology when desired. OLSR inherits the concept of forwarding and relaying from the HIPERLAN version 1 MAC layer protocol, which is standardized by ETSI. Within NRLOLSR, additional optimized flooding algorithms were added in addition to MPRs in order to support experimentation of multicast routing approaches discussed later in this document.

2.2.2 MANET-OSPF

Since Phase I of INSC, the US and other participants within the IETF have established a design team for the development of MANET extensions to OSPF. This was supported by both the MANET and OSPF Working Groups (WGs) within the IETF. Some US ONR-funded work to support this effort by Boeing has been made available publicly and to the IETF community [20].

The experimental MANET-OSPF prototype code [21] developed by Boeing was used within INSC Phase II to examine basic performance of the protocol in both the Quagga routing suite [22] under Linux and within the GTNETS simulator [23]. The code implements a number of evolving algorithms and approaches being considered for IETF standardization. This has allowed the INSC communities to take an early look at the potential of this protocol and its technical options under design consideration.

In 2003, Boeing developed an adaptation of OLSR to fit it within the OSPF framework, and called it "Wireless OSPF" [24]. This work showed that a periodic, unacknowledged flooding technique based on the principles of OLSR could, in some mobile network scenarios, reduce protocol overhead by an order of magnitude. Additional quantitative results can be found in [20].

In 2004, the OSPF Working Group, in cooperation and with assistance from the MANET WG, agreed to commence work on a MANET extension for OSPFv3 (for IPv6), and formed a design team to come up with a recommended approach to the extension. The Working Group decided to focus on protocols that used reliable, acknowledged flooding, rather than periodic, unacknowledged flooding found in OLSR and the initial Wireless OSPF proposal, because reliable flooding better matches the existing design framework of OSPF.

A Boeing technical report [20] is available that was partially sponsored by the US Navy provides a comparison of many MANET-OSPF scenarios and options and also compares it against previous OLSR work. It showed similar performance between to the two protocols with some scaling advantages to unreliable flooding of topology information as done in OLSR. It also demonstrated that the major improvement in MANET-OSPF design is based upon the potential for reduced adjacency advertisement when using the Manet Designated Router (MDR) approach. This will allow MANET-OSPF to scale to potentially larger numbers of routers within a single routing area (e.g. 100) than was previously possible with OSPF.

2.2.3 Small network comparisons of MANET-OSPF and OLSR

A direct comparison of the Boeing MANET-OSPF code and NRLOLSR was conducted on the US-developed Mobile Network Emulator (MNE) operating over 2Mbps 802.11b Wireless LAN, with the purpose of evaluating the relative performance of each protocol. This scenario chosen was a 10-node network with a random motion model (identical for each protocol, however), and a traffic scenario of Many-to-One with each node sending MGEN data to a gateway node. The amount of traffic starts out low, but is increased to medium loading and then past the point of congestion. Since this is a direct comparison, an effort was made to ensure that the protocol parameters were as close as possible to one another. Hello intervals and timeouts were set the same (2 seconds and 16 seconds, respectively). Both protocols were run in a full link state mode, and hysteresis was disabled on NRLOLSR, as it is not currently supported in the MANET-OSPF implementation. MANET-OSPF was also set to use the MPR algorithm instead of the MDR algorithm for controlling flooding, because the MDR mode was unfortunately not working in the quagga-based implementation at the time of the experiment. The results of the experiment are shown in the following figures.

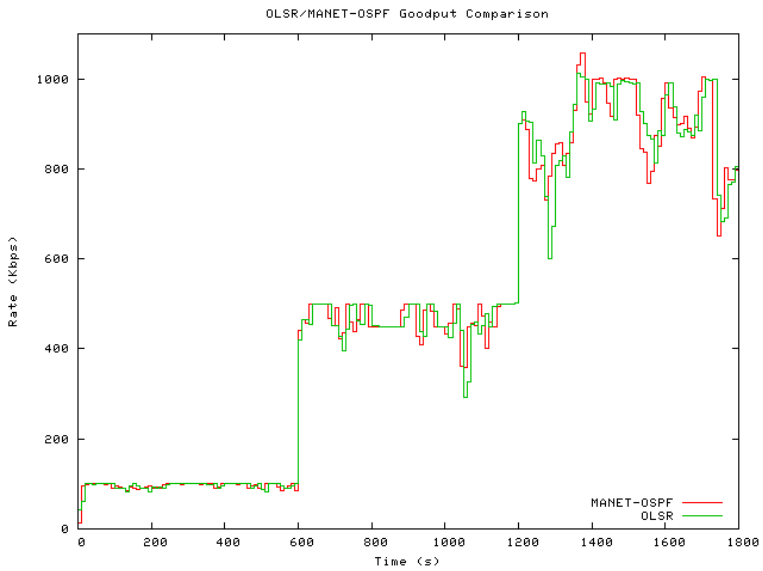

Figure 1: Rate plots for OLSR and MANET-OSPF

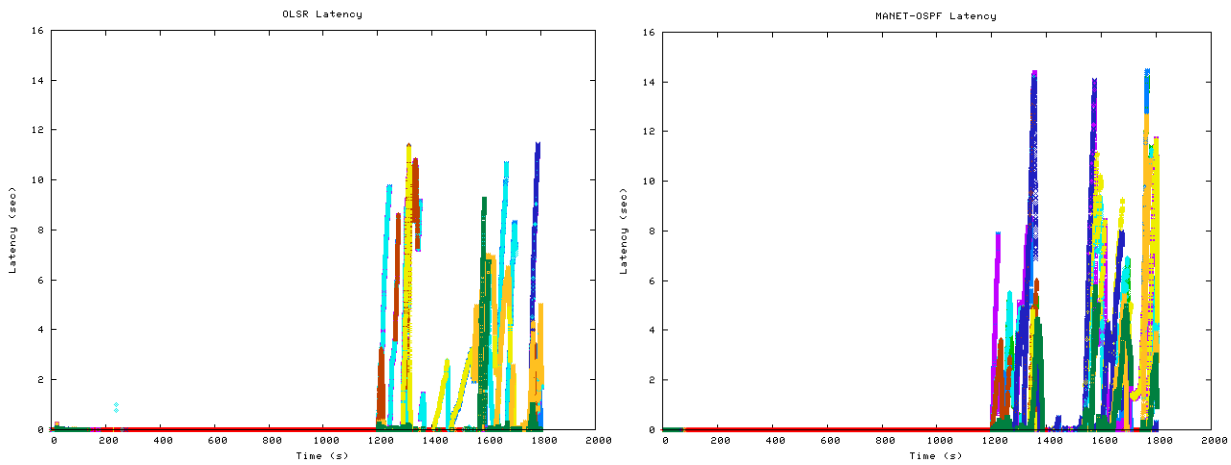

Figure 2: Latency plots for OLSR and MANET-OSPF

It should also be noted that the large drop in goodput in Figure 1 at around 800 seconds (in the middle of the medium loading period) is unavoidable, as it is due to a temporary network partition that is part of the mobility model. Both protocols are able to recover from this partition successfully.

As you can see from the graphs, the aggregate performance of MANET-OSPF and OLSR is very similar in this small network scenario. The rate plots have only slight differences, and the latency of both protocols is dominated by the retransmission buffers in the WLAN cards. It is expected, and it has been shown in simulation, that the performance difference of these protocols is more visible when the networks are scaled up to a larger number of nodes. MANET OSPF was also run in a variety of modes, including differential Hellos and partial link state, and the performance difference for this size scenario was negligible.

When this scenario was run without disabling hysteresis on NRLOLSR, the performance characteristics were quite different, with OLSR having about twice as much loss as MANET-OSPF. Hysteresis results in a slower reaction to link changes per sensing period, but it is important to prevent route flapping and instability in real-world operation, with hidden terminal problems, channel fading, etc. This further demonstrates the importance of understanding each parameter of a given protocol and test conditions during post analysis.

2.2.4 AODV vs. OLSR

A direct performance comparison of OLSR and AODV in a number of network and traffic configurations was conducted on the UK Large Network Emulator (LNE) in a 2Mbps Wireless LAN configuration using a variety of 16 node mobile networks. The complete set of experimental results is detailed in [26].

The protocol implementations tested were IPv4 versions of NRLOLSR and Uppsala University AODV (AODV-UU) [25]. Although AODV is a reactive protocol, the specification allows the option of Hello packets to be supported for determining continued neighbor connectivity while a route is active. This option is implemented by AODV-UU. In addition, AODV-UU has a mode where Hello packets are permanently transmitted even if there is no traffic to send (referred to as AODV+H). This mode is used to help detect link failures when the underlying radio hardware is incapable of doing so reliably. It was thought that this mode may also lower the time to initially discover a route and was included in the experiments for comparison. Default protocol parameters were used for all protocol variants except for the Hello interval, which was tuned to 5 seconds for both OLSR and AODV+H.

Traffic was needed to evaluate the performance of each protocol under mobility. In addition, since AODV is a reactive protocol, traffic is needed to coax the protocol into producing full routing overheads. Finally, the actual traffic profiles used contained periodic intervals of inactivity to take into account AODV's behavior of timing out inactive routes between bursts.

It was found that OLSR had higher routing overheads than AODV and AODV+H in all network types, because it proactively maintains routes even when there is no traffic to transfer. Routing protocol overheads were highest for all protocols in the line network topology, since it is a worst-case scenario for both protocols. For OLSR, this is because all nodes except the ends of the line are chosen to be MPRs and therefore must forward routing control information. For AODV, when traffic was sent between nodes at the ends of the line, all the intermediate nodes are involved in route discovery and maintenance, thus maximizing overheads. In the case of the mesh network, the OLSR MPR set is much smaller due to the increased level of connectivity in the network, while nodes not on active routes in AODV do not have to issue route maintenance packets. The tradeoff of lower AODV routing overhead was demonstrated by the resulting delay in the delivery of the first packet in a new traffic flow. As OLSR always maintains routes, this figure was in the millisecond region, whereas it could be on the order of seconds for AODV. As expected, AODV+H sat somewhere in the middle of these results by virtue of

its increased overheads. Goodput was found to be reasonably comparable between routing protocols in the same experiment and the line topology was again found to produce the worst results, due to the higher number of collisions produced by the increased overhead over longer routes with no scope for route diversity. Further details may be found in [26].

2.2.5 OLSR/OSPF Gateway Approaches

The Internet is structured as a collection of inter-connected networks of various sizes called Autonomous Systems (AS) or domains. These domains are managed independently one from the other, although they must all follow the Internet standards in order to ensure they can communicate between one another.

OLSR and OSPF [5] are both Internal Gateway routing protocols (IGPs), specialized in routing inside a single domain. Within the INSC infrastructure, OLSR MANETs were shown to have reachability to one another via the OSPF-based WAN by treating them as stub networks with a unique aggregate prefix, which was in turn a part of the aggregate prefix of the Coalition LAN (CLAN). This may work in many instances, but for more general interoperability between OLSR and OSPF, we need something more complex. Two methods were investigated by CELAR (FR) for interconnecting OLSR and OSPF domains. The first method is to use a different type of routing protocol that is hierarchically *above* IGP routing. This different type of routing is called External Gateway Protocol (EGP), and specializes in routing between different domains. The predominant EGP protocol is BGP, the Border Gateway Protocol [6]. The first method will therefore use BGP to interconnect OSPF and OLSR.

Additionally, OSPF and OLSR both incorporate mechanisms to exchange routing information with other routing protocols. The second envisioned method therefore made use of these mechanisms to interconnect OSPF and OLSR, without the use of a third-party protocol. OLSR features a simple and efficient mechanism to import routes coming from another routing protocol in the form of Host and Network Association (HNA) messages. With these messages, an OLSR node can advertise its connectivity to non-OLSR hosts or networks. For instance, if an OLSR node is connected via another interface to an OSPF network, it can periodically generate and transmit HNA messages including the OSPF network's IP prefixes. Routes to the OSPF network will then be included in routing tables at all OLSR nodes. Similarly, OSPF uses Link State Advertisement (LSA) message types 5 and 7 to import routes coming from another routing protocol. These messages advertise routes that are external to the OSPF network, which are then included in OSPF-driven routing tables. This method of using internal mechanisms to interconnect OLSR and OSPF seems a more appropriate solution to the problem, as it is more simple and efficient, and it does not require a third routing protocol. This method has been successfully demonstrated on the French testbed. For more information, please see [27].

2.2.6 Other Unicast Routing Protocols

IETF work regarding MANET protocols concentrates on the IP layer, though the same algorithms may be applied at the MAC layer to produce similar results. T3 was aware of

work going on in this area, but there was little inter-PO collaboration and testing of these types of systems. We agreed to concentrate most of our work on evolving Internet Standards items.

Here we provide a brief description of specific related GE (FGAN) research carried out involving the design of MANET protocols below the IP layer or between IP and MAC layer. Two nonstandard protocols have been designed, the *MANET Forwarding Protocol (MFP)* and the *Wireless Network (WNet)* MANET framework. Both protocols take advantage of the inherent broadcast capability of wireless link networks. They both implement forwarding of IPv4 and IPv6 unicast and multicast packets in MANETs, conceiving unicast as a special case of multicast transport with a single receiver.

As far as the IP layer (and above) is concerned, a MANET using MFP or WNet looks like a single Ethernet segment (see Figure 3, blue network). This allows for an intrinsic interoperability with any IP layer routing protocol and simplified IP configuration – only the gateway node between the wired and the wireless subnets must be able to do IP routing. The wireless nodes behave like Ethernet hosts and can even take advantage of IPv6 autoconfiguration. The MANET can easily be used as a transit network by adding another wired gateway/router and running a routing protocol like OSPF on the gateway hosts.

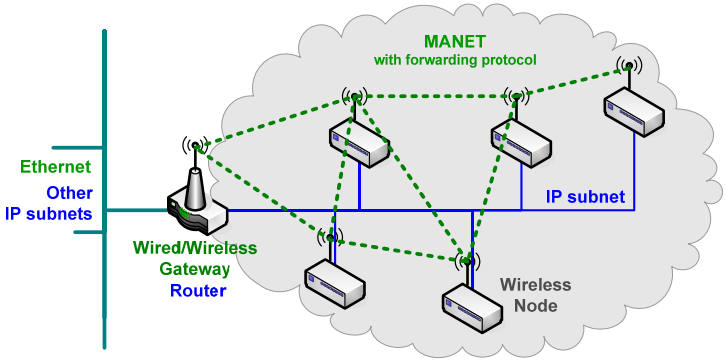

Figure 3: MANET network using a forwarding protocol, as seen from the MAC layer (green) and from the IP layer (blue)

MFP has been designed as a simple protocol with the ability to forward IPv4 and IPv6 packets in small to medium-sized MANETs. It uses a broadcast emulation to flood route request packets in the MANET and a directed forwarding algorithm to transport unicast and multicast data, embedded in special MFP multicast packets. Route discovery is on demand, but existing links are proactively maintained. Route calculations use a hop count and link quality based metric, taking into account the fluctuating connectivity of wireless links. MFP also includes a security concept which uses private/public key encryption to protect the data and control flow against non-trusted nodes. This security concept requires that the public keys of the participating nodes be pre-distributed to all legal member nodes of the MANET.

Detailed protocol implementation and testing information can be found in [28]. A prototype implementation for Linux with kernel 2.4 and 2.6 and Wireless LAN hardware, supporting IPv4 and IPv6 has been realized and tested.

The MFP Linux implementation is being tested in both emulation and live field tests using the “line” motion model. Both test traffic and real applications including VoIP and video streaming have been run over MFP. Emulation tests demonstrated the principle functionality of the protocol in small-scale MANETs and field tests have confirmed the functionality of the protocol in real-life scenarios. Joint mobile testing between FGAN (GE) and CELAR (FR) demonstrated that an MFP network can interconnect with an OLSR network over the INSC WAN, using both test traffic and real applications. This worked as expected, due to the network transparency of both protocols. Performance testing larger networks and higher rates of mobility, and performance comparison with other MANET protocols will be future work.

In contrast to MFP, WNet forwarding is based on the principles of the OLSR protocol, using Multi-Point Relays for efficient flooding [29]. One focus of the framework is to support efficient multicast communication. WNet implements extensions concerning quality and priority based forwarding, quality of service, and congestion management. Provisions are made for power awareness and security. Since the framework is positioned on the MAC layer, it has direct access to device parameters and can therefore determine link and node attributes. These are used to calculate link qualities that influence the forwarding decision, leading to a quality-based routing mechanism. The WNet implementation has been tested using a wireless testbed with up to eight nodes. Tests have been performed successfully with video streams of up to 1.2 Mbps over three hops, using 802.11a adaptors running at 6 Mbps. In addition, it is regularly used on multiple hosts in the multi-robot system at FGAN/FKIE (GE) with parallel transmission of video stream, sensor data, position information and remote control commands.

2.3 Simplified Multicast Forwarding Work

A significant technological improvement of MANET work done under INSC since Phase I has been the inclusion and testing of a MANET multicast routing solution. A common approach that is progressing within the IETF and that was examined by various POs was the Simplified Multicast Forwarding (SMF) protocol.

SMF is designed to have limited applicability as a forwarding mechanism for multicast packets within MANET routing areas. In addition, it provides mechanisms to support interoperability with a connected wired infrastructure. SMF uses a simplified forwarding mechanism that delivers multicast packets to all MANET multicast receivers within a MANET routing area. The core design does not use receiver specific group information, instead favoring a reduced complexity and state maintenance within the mobile topology, but such extensions may follow in later specifications. The design accounts for the unique nature and behavior of MANET interfaces and takes advantage of efficient relay set algorithms previously designed and applied in the MANET unicast routing control plane. The present SMF IETF Internet Draft [10], edited by the Task

Leader (US/NRL) with contributions from CRC, describes the SMF forwarding and duplicate detection mechanisms in detail, describes optional SMF neighborhood discovery mechanisms, and defines several efficient relay set algorithms that have been implemented in conjunction with SMF.

Early US [29] and CA SMF prototypes were investigated within INSC Phase II testbeds and related field experiments. A Task 4 field experiment (GE) used both NRLOLSR and SMF to successfully demonstrate black routing functionality amongst mobile platforms. Prototype implementation and testing done by the US at NRL and CA at CRC demonstrated that SMF can support a variety of flooding techniques, from classical flooding (i.e., each node forwards each multicast packet once) to more advanced Multi-Point Relay (MPR, also used in OLSR) and Connected Dominating Set (CDS) algorithms including the essential CDS and MPR-CDS variants.

2.3.1 Classical Flooding

The simplest design often conceived and adapted for MANET packet flooding we designate as the "classical flooding" (CF) algorithm. In CF, each participating forwarder node is required to rebroadcast packets intended for dissemination once and only once. This approach is extremely simple and only requires only some means of duplicate packet detection (DPD) and a basic forwarding mechanism. However, it is well known that using CF, especially within dense networks, results in a significant number of redundant transmissions, an effect often referred to as the broadcast storm problem [31]. Within wireless multi-hop networks, direct contention and interference is often experienced beyond the single hop interface, and reducing unnecessary channel contention within a MANET can also significantly improve network performance. Therefore, minimizing the number of required relay nodes is a heightened design goal in this environment. Unfortunately, reducing the number of relay nodes in a MANET environment may also decrease the robustness of packet delivery in a mobile topology. There exists a design tradeoff between relay efficiency and delivery robustness that is scenario and system dependent and should be considered carefully.

2.3.2 Efficient Relay Set Algorithms

At a theoretical level, work in the area of minimizing packet forwarders, or relay node sets, is often related to basic graph theory problems. In graph theory, a dominating set (DS) for a graph is a set of vertices that, along with their neighbors, constitute all the vertices in the graph. A connected DS (CDS) is a DS where the subgraph induced is connected. A minimum CDS (MCDS) is a set such that the number of vertices is the minimum required to form a CDS.

Finding a small dominating set is one of the most fundamental problems of traditional graph theory and is often related to the problem of optimizing flooding algorithms in MANET routing protocols. Finding an MCDS in a given graph is known to be NP-hard [32]. These basic static graph theory issues are important to apply in developing efficient relay sets, but in addition, MANET relay set designs require distributed and dynamic operation. To better explain the design requirement, the SMF specification

formulated the following characteristics desired of an effective MANET flooding algorithm solution for use in SMF:

- A resultant cover set that is small compared to the total number of nodes as the network scales in size and density.
- A robust approach somewhat resilient to network mobility and link dynamics.
- A cover set election/maintenance mechanism that is lightweight, distributed, and adaptive in nature.

Five algorithms have been implemented and compared within the NRL prototype implementation of SMF. In order to not require a redundant neighbor discovery protocol, the SMF relay set election information is obtained from the NRLOLSR implementation running in parallel with SMF. In the absence of NRLOLSR, the SMF implementation will need to execute its own neighborhood discovery protocol in order to collect the necessary link symmetry and 2-hop information needed in a wireless environment. The five algorithms currently supported are:

- Classical Flooding (CF)
- Multipoint Relay (MPR)
- Non-Source Specific MPR (NS-MPR)
- MPR Connected Dominated Set Extension (MPR-CDS)
- Essential Connected Dominating Set (E-CDS)

2.3.3 Flooding Algorithm Comparison

NRL has executed both mobile emulation (up to 10 nodes) and simulation (up to 25 nodes) experiments of these SMF flooding algorithms under various multicast traffic patterns and mobility models. Some results of these studies follow.

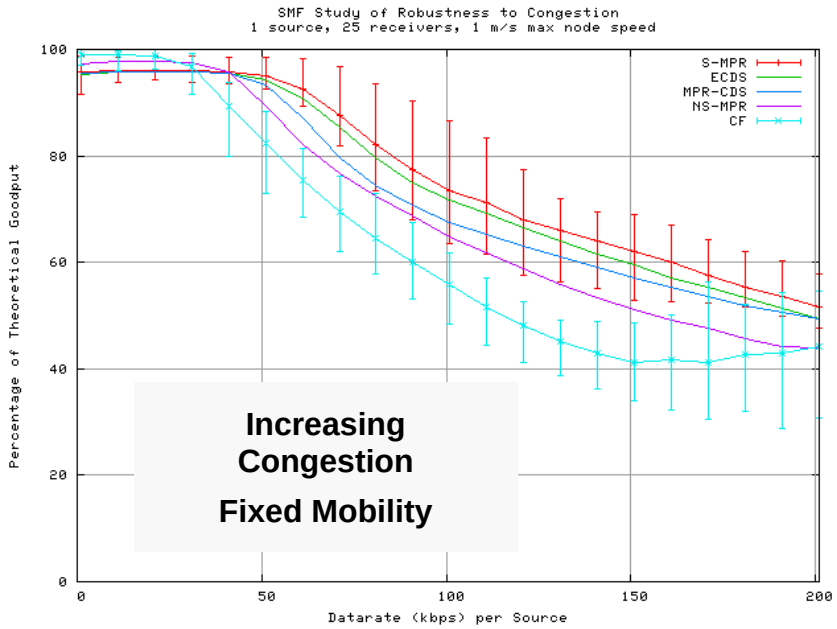

Figure 4: Simulation study of SMF robustness to congestion

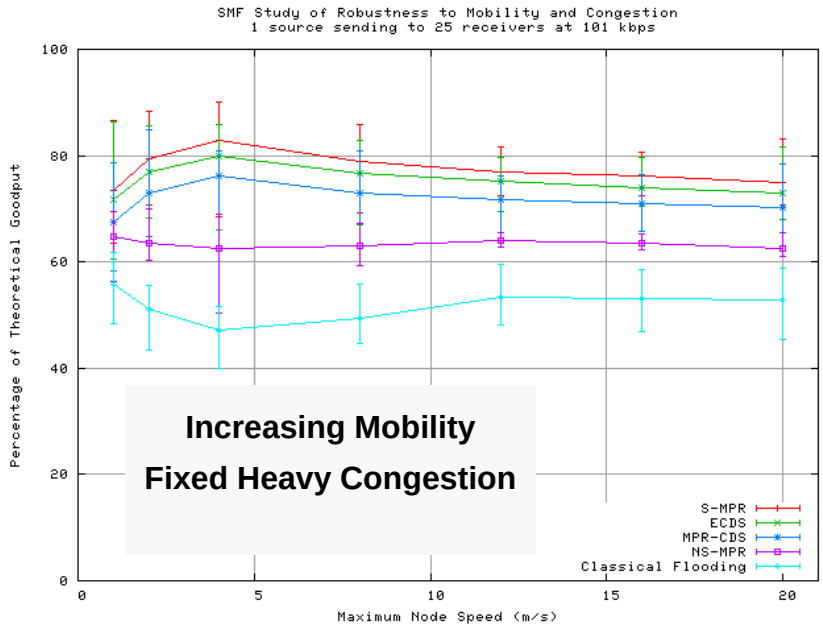

Figure 5: Simulation study of SMF robustness to mobility

Figure 4 and Figure 5 show the results of ns2 simulation studies of SMF robustness to congestion and mobility. These results show that more efficient relay set algorithms such as E-CDS and S-MPR perform very well under congestion and mobility compared to classical flooding. NS-MPR shows a consistently lower performance than the other three algorithms, though it is still a large improvement over CF.

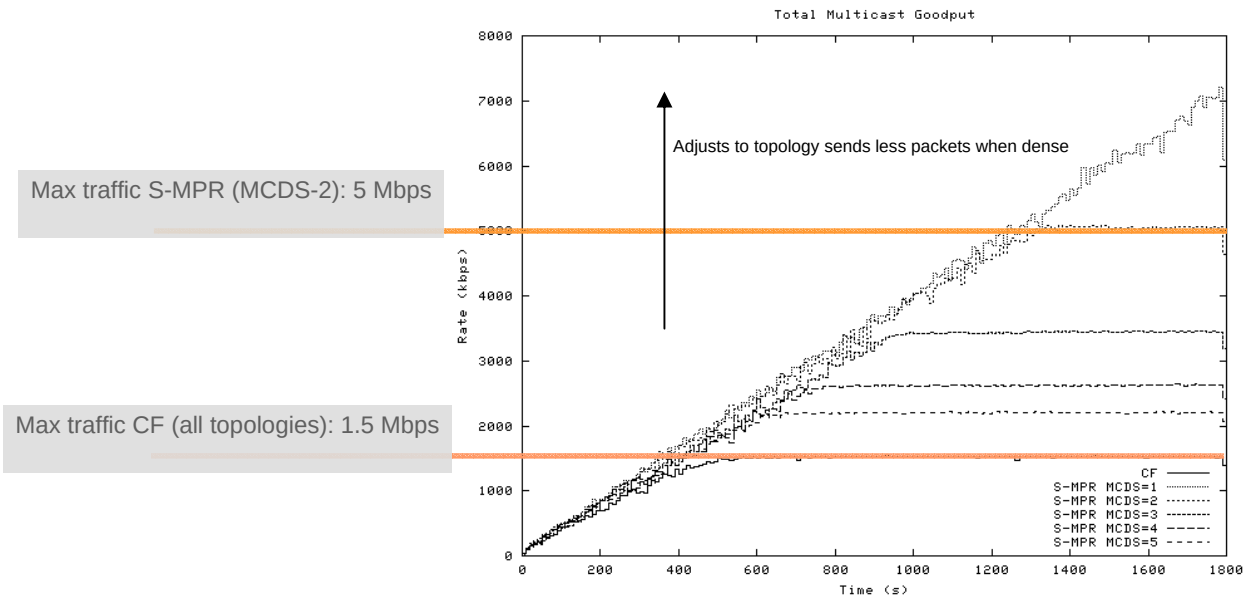

Figure 6: Emulation study of S-MPR flooding with different node densities

The above results shown in Figure 6 represent an emulation test done during INSC Phase II to examine the performance of SMF optimized flooding (e.g. S-MPR) as network density is changed. The MCDS degree indicates the number of nodes needed to form a MCDS relay set. Smaller numbers represent more dense MANETS, while larger numbers represent more sparse topologies. This shows that even in a small multicast network (10 nodes), significant additional user traffic can be supported with the use of an efficient relay set algorithm.

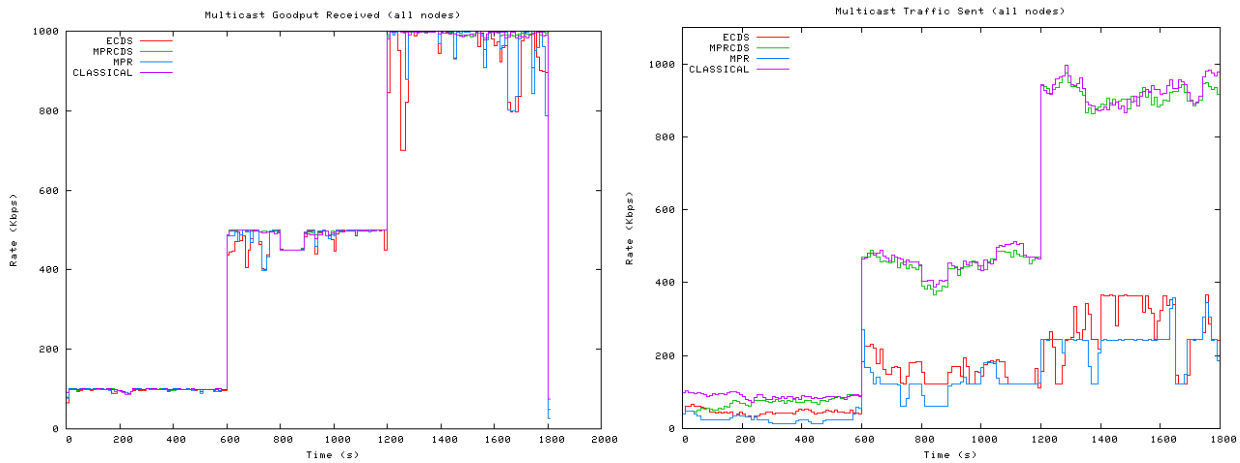

Figure 7: Emulator study of SMF overhead

The results in Figure 7 show goodput in a 10-node mobile emulation experiment along with the amount of network loading required to obtain this level of goodput. It should be noted that the large drop in goodput at around 800 seconds is unavoidable, as it is due to a temporary network partition that is part of the mobility model. SMF is able to recover from this partition successfully. These results show that more efficient relay sets such as S-MPR and E-CDS result in far less loading of the network than CF and

MPR-CDS. In fact, while MPR-CDS and CF are congested at the highest level of traffic, S-MPR and E-CDS are still able to support additional traffic. The results also show that while S-MPR and E-CDS are far more efficient than CF and MPR-CDS, they are also more susceptible to packet loss under motion. NS-MPR was not tested in this scenario. More SMF test results may be found in [33].

In addition to performance tests, several multicast applications were also run successfully over MANETs using SMF. These applications included voice-over-IP (VoIP), video streaming, whiteboard, file transfer, and multicast chat. Additionally, the US ran some experiments using Nack-Oriented Reliable Multicast (NORM) [34]. Based on previous Multicast Dissemination Protocol (MDP) [35] work, NORM is a transport layer protocol that makes use of the concepts of Negative Acknowledgements (NACKs) and Forward Error Correction (FEC) to send multicast data reliably and efficiently. NORM was used to improve robustness of VoIP, video streaming, file transfers, and chat applications over MANET networks when using less robust SMF algorithms such as MPRs.

2.4 Other MANET Multicast Protocols

2.4.1 MOLSR for IPv4

The Multicast Optimized Link State Routing (MOLSR) protocol [36] is an extension to the OLSR unicast routing protocol. It supports group-based multicast, which may be more efficient than flooding the information to all nodes as SMF does, depending on the scenario. MOLSR takes advantage of the topology information gathered by the OLSR protocol with its Topology Control (TC) messages and uses that information to build multicast trees for any source/multicast group pair. This is done in a distributed manner and provides shortest routes from the source to the multicast group members. The trees are updated whenever a topology change is detected.

MOLSR works even when some nodes are not multicast-capable, provided that multicast-enabled nodes are able to offer the minimal connectivity between the source(s) and the members of the multicast group. The multicast routing table provides the shortest routes to all multicast-capable nodes in the network using only the multicast-capable routers. The calculations are done in the same way as they are done for the OLSR unicast routing table, with a slight modification. The MPR set must be calculated in such a way that, 2-hop multicast capable nodes are covered by 1-hop multicast capable nodes when it is possible. Multicast-capable nodes are chosen preferably over other nodes. The multicast routing table is updated whenever the OLSR routing table is recalculated, or when a new multicast node is discovered, or disappears.

The Internet Group Management Protocol (IGMP) is used by hosts to report their multicast group joins and leaves to neighboring multicast routers. It is also used by multicast routers to discover group members. According to the IGMPv2 and IGMPv3 standards, IGMP is required to be implemented by any host wishing to receive IP multicast packets. However, in a wireless network such as a MANET, the use of IGMP may lead to some problems. More precisely, the elimination procedure of queries as

described in IGMP is problematic in a wireless context. Therefore, MOLSR makes use of Wireless IGMP (WIGMP). WIGMP is only concerned with the exchanges between hosts and routers to determine group membership, and the multicast routing protocol is in charge of building and maintaining a multicast structure. WIGMP uses the same messages specified as in IGMPv3, and the host IGMP also remains unchanged.

In addition to performance testing, the INRIA MOLSR implementation [37] has also been used for functional application testing of VoIP and video streaming. For further details, please see [38] and [39].

2.4.2 MFP and WNet

The MANET Forwarding Protocol (MFP) developed by GE (see p. 11) was designed to support efficient multicast data transfer in MANETs. Like MOLSR, MFP supports real group-based multicast, rather than flooding. This is done by attaching a list to each packet, containing the path which the packet should traverse. The robustness of this method under high mobility requires further investigation. Multicast MFP tests were performed both in emulation and field trials. Applications run over MFP included multicast video conferencing, chat, and an application to disseminate GPS position information. WNet is also primarily designed to support efficient multicast data transport. In contrast to other multicast-enabled protocols, WNet offers an optional link layer retry mechanism for multicast packets in Wireless LAN. WNet multicast operation is part of the installation in the multi-robot system at FGAN (GE), described earlier.

2.5 Multicast Protocol Comparison

The UK performed a large emulation experiment comparing a number of IPv4 MANET multicast protocols in a number of network and traffic scenarios. The Large Network Emulator (LNE) was configured in a 2Mbps Wireless LAN mode and the metrics used to evaluate performance were total overhead and total traffic delivery.

The protocols used in the experiments were:

- Unicast: as a baseline, NRLOLSR was used as an underlying unicast protocol to support N multiple unicast traffic flows to simulate a multicast delivery to N listeners. With this approach, not all nodes in a MANET need receive multicast packets if they are not listeners.
- NRLSMF with Classical Flooding (CF), with NRLOLSR running as the unicast protocol to provide a fair comparison with other protocols that also provide a unicast capability.
- NRLSMF with CF, without a unicast protocol, was included to cover the possibility of multicast-only networks.
- SMPR: NRLSMF with Multipoint Relay set provide by NRLOLSR.
- INRIA MOLSR, a group-based multicast solution, rather than a simplified flooding approach. Instability in the implementation limited the number of successful

experiments that were possible with MOLSR. In particular, few experiments with multiple senders were possible.

The metrics used to evaluate performance were total overhead and total traffic delivery. Total traffic delivery represents the percentage of unique packets received at the listeners compared to the number of packets originally sent, and then averaged across all listeners. In this way, delivery against network loading can be assessed for each protocol in each network scenario.

The experiments were conducted in 16-node (mobile and static) and 40-node (static) networks using the line, tree, cluster, and mesh network topologies described earlier. The traffic profiles used in the experiments include:

- 1/2_n_m_a: ½ of the nodes in the middle of the network sending flows with all nodes as listeners, e.g. distribution of centralized situational awareness
- 1_1/2n_c: One node on the network sending flows with half of the closest nodes as listeners, e.g. multicast chat
- 1_1/2n_f: One node on the network sending flows with half of the furthest away nodes as listeners, e.g. worst case generalized multicast chat
- a_a: All nodes sending flows with all other node as listeners, e.g. distributed situational awareness

From the many experiments that were conducted, the following were extracted to demonstrate that no one protocol outperforms all others in all situations.

2.5.1 16-Node Static Networks with 1/2n_m_a Traffic Profile

This set of experiments clearly demonstrates the inefficiency of using multiple unicast flows to deliver multicast traffic. Figure 8 shows that multiple unicast flows creates much higher overhead than multicast delivery, while Figure 9 shows that this increased overhead leads to lower traffic delivery. Of the other protocols, SMPR multicast has the least overhead, as it is more efficient at relaying packets around the network. This is coupled with overall delivery as good as, or better than, any of the other protocols.

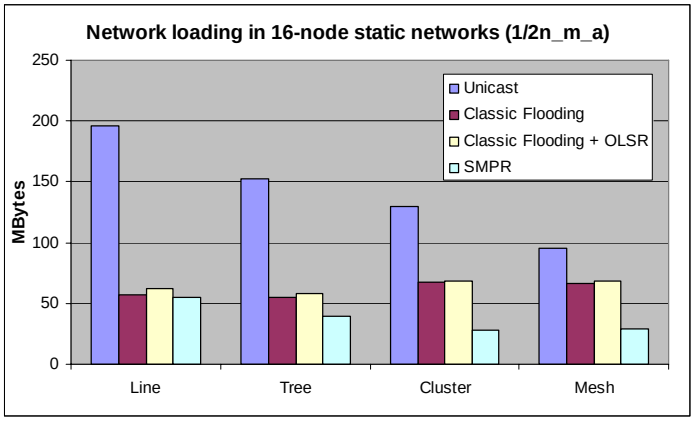

Figure 8: Network Loading in 16-Node Static Networks (1/2n_m_a)

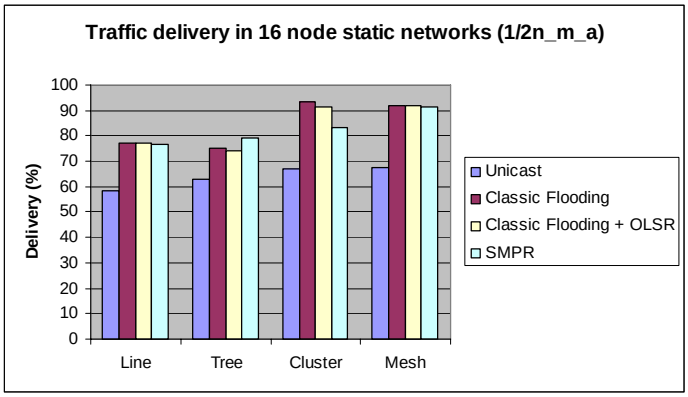

Figure 9: Delivery of Traffic in 16-Node Static Networks (1/2n_m_a)

2.5.2 16-Node Static and Mobile Networks with 1_1/2n_f Traffic Profile

In a network with faraway receivers, the benefits of directed forwarding are diminished, as many of the nodes in the network must join the multicast tree to forward packets to their required destinations. Thus, the overhead of MOLSR is equivalent to the other multicasting techniques as seen in Figure 10, with similar delivery results (Figure 11) in the static networks (mobile MOLSR experiments were not conducted).

It can be seen that when the protocols are performing well against mobility, they have slightly higher overheads than in the static case (e.g. mesh and mobility networks). When they are performing less well (e.g. line and tree networks), they have similar overheads due to the reduced connectivity in the network, which thereby reduces the amount of overhead present. This is consequently mirrored in the lower traffic delivery results against the static network.

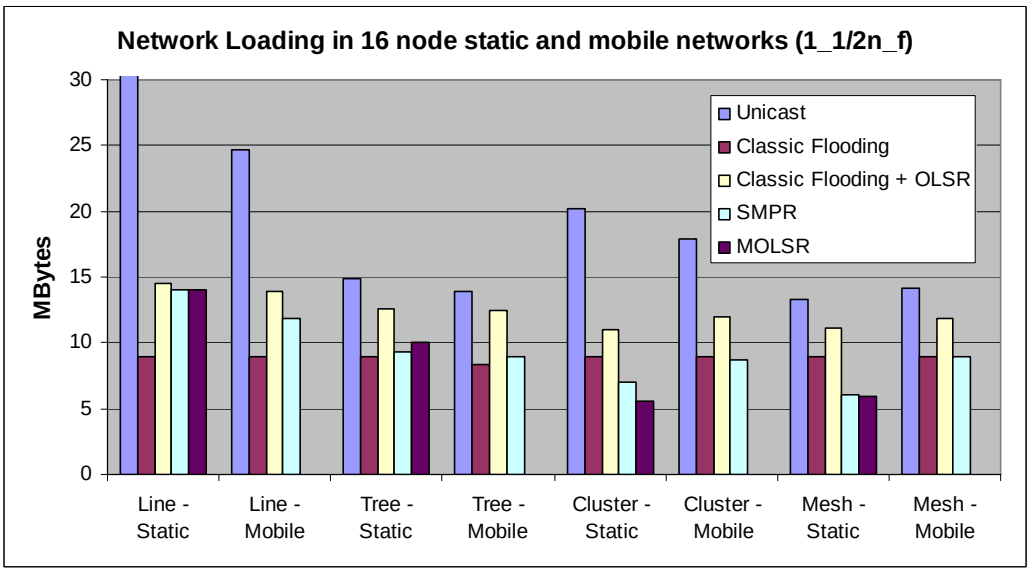

Figure 10: Network Loading in 16-Node Static and Mobile Networks (1_1/2n_f)

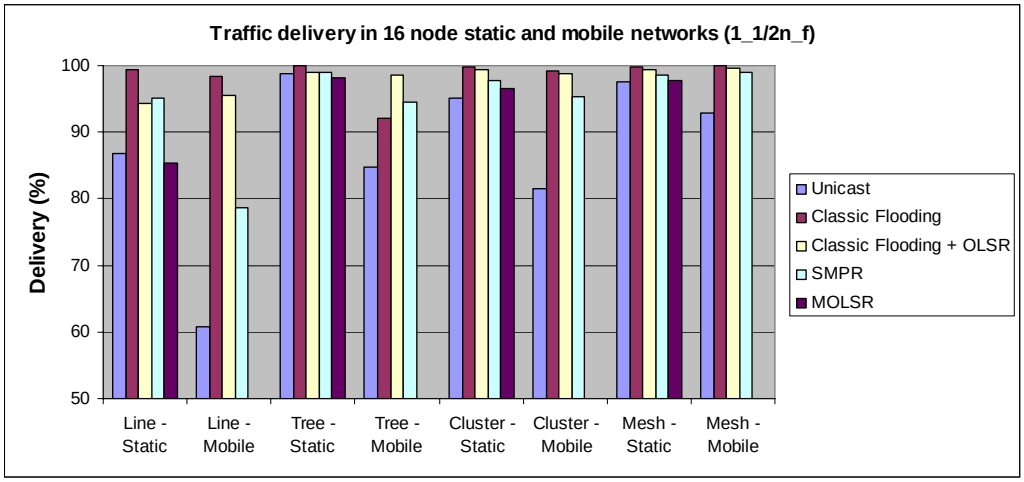

Figure 11: Delivery of Traffic in 16-Node Static and Mobile Networks (1_1/2n_f)

2.5.3 16-Node Static Networks with 1_1/2n_c Traffic Profile

Figure 12 shows how multicast with nearby neighbors favors the directed forwarding of MOLSR, which has significantly lower overhead than any other protocol. Traffic delivery (Figure 13) is very high across all protocols, as there are few hops separating nodes, thus reducing the possibility of collisions even in the line network.

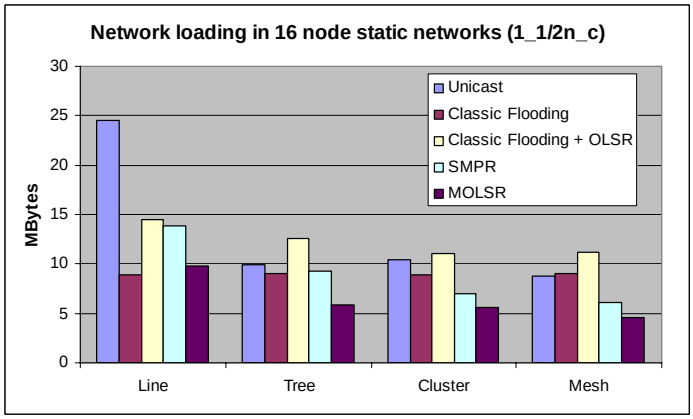

Figure 12: Network Loading in 16-Node Static Networks (1_1/2n_c)

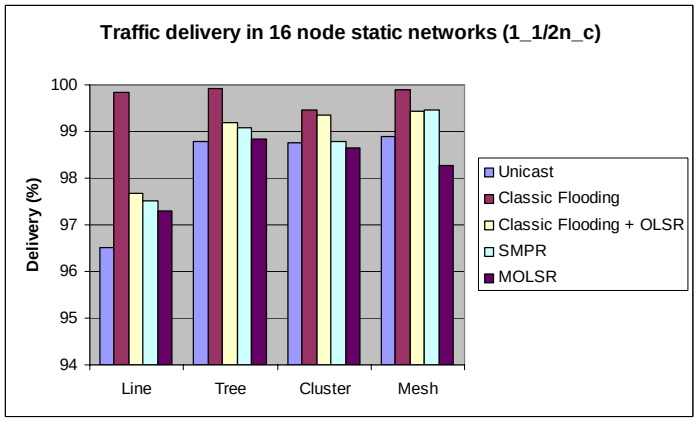

Figure 13: Delivery of Traffic in 16-Node Static Networks (1_1/2n_c)

2.5.4 16- and 40-Node Static Networks with a_a Traffic Profile

Figure 14 and Figure 15 demonstrate the major increase in network overhead that each protocol incurs when the test network is scaled from 16 to 40 nodes. The increased amount of overhead in the cluster and mesh networks for the multicast protocols is probably an indication of far more successful traffic delivery than for multiple unicast flows. However, the general trend of 400-800% increase in overheads compared to a 250% increase in the number of nodes raises some concern over the scalability of all the protocols present.

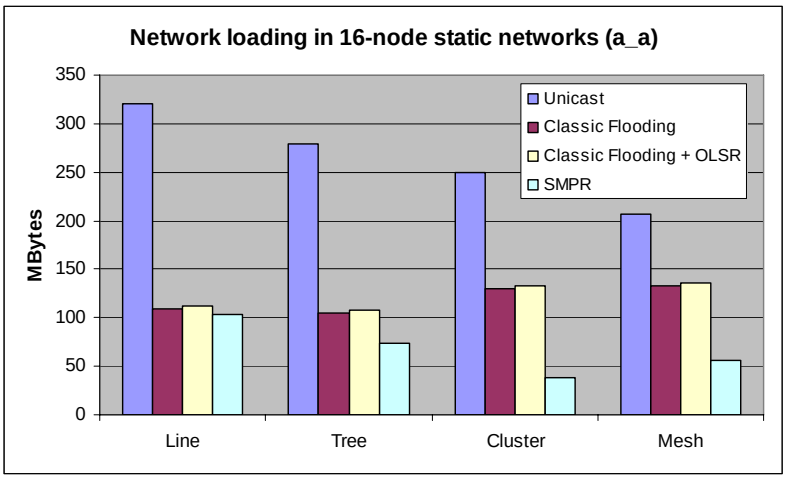

Figure 14: Network Loading in 16-Node Static Network (a_a)

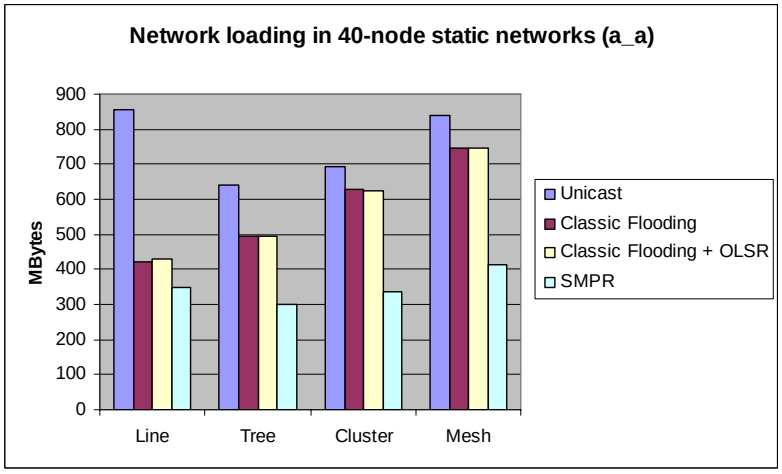

Figure 15: Network Loading in 40-Node Static Network (a_a)

The general trend for the multicast protocols is to cause significantly higher network loading in the cluster and mesh networks, since they are making use of the increased route diversity to successfully deliver more traffic (see Figure 16 and Figure 17). For instance, SMF CF with unicast OLSR will cause a packet to be delivered to a receiver multiple times in a highly meshed network; therefore, if some of the copies were previously lost due to collisions, there is still a chance that one of the copies will succeed, thus trading increased network loading for delivery resilience. In the case of

the unicast protocol, the amount of loading in the 40 node networks is actually saturating the network, resulting in very poor levels of traffic delivery. As expected, delivering multicast traffic in this way is very inefficient since the same information is replicated 16 or 40 times at each source node, rather than once as with multicast.

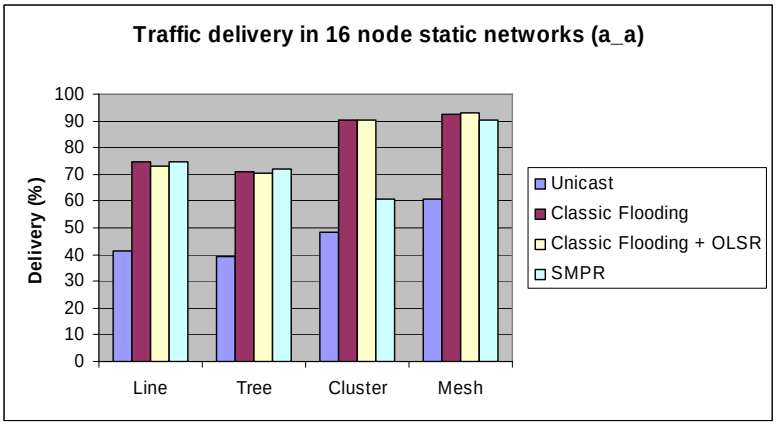

Figure 16: Delivery of Traffic in 16-Node Static Network (a_a)

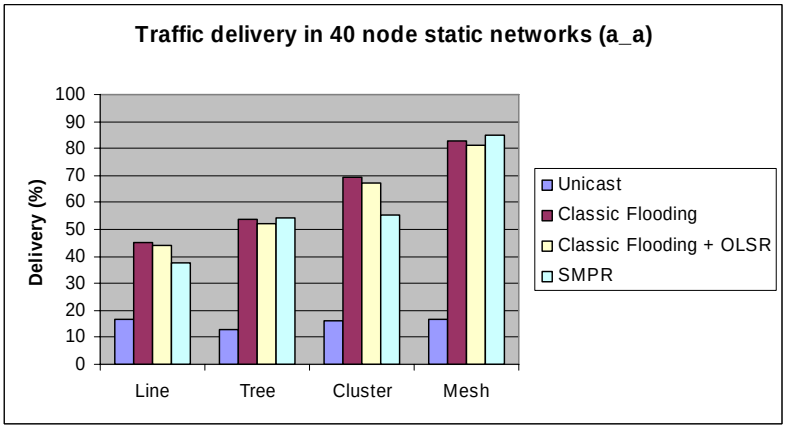

Figure 17: Delivery of Traffic in 40-Node Static Network (a_a)

2.6 Multicast Gateway Functionality

The multicast protocols discussed thus far deal with how to disseminate multicast data throughout the MANET. In order to be more useful in a broader range of scenarios, we need to be able to get multicast data to and from a more fixed infrastructure. For unicast, we have a relatively simple problem of distributing routes between unicast routing protocols. The actual forwarding of unicast packets is done by the OS, using the supplied routes. Multicast gateways are more complex, as they are required both to join multicast groups on behalf of the MANET, as well as to forward multicast data packets between the networks themselves.

The INSC network setup, shown in Figure 18, is a fairly typical network setup. The MANET is connected as a stub network to a larger, more fixed infrastructure. Each red-side MANET is connected in this manner. We will assume that SMF is running in the MANET, though other MANET multicast protocols could be used as well. The MANET

gateway has one interface connected to the MANET, and another connected to the larger infrastructure, which is running Protocol Independent Multicast (PIM) [40] [41] to support multicast data. An IPSec machine separates the red and black routing domains to add security to the architecture, but that is not relevant to the problem of a MANET multicast gateway.

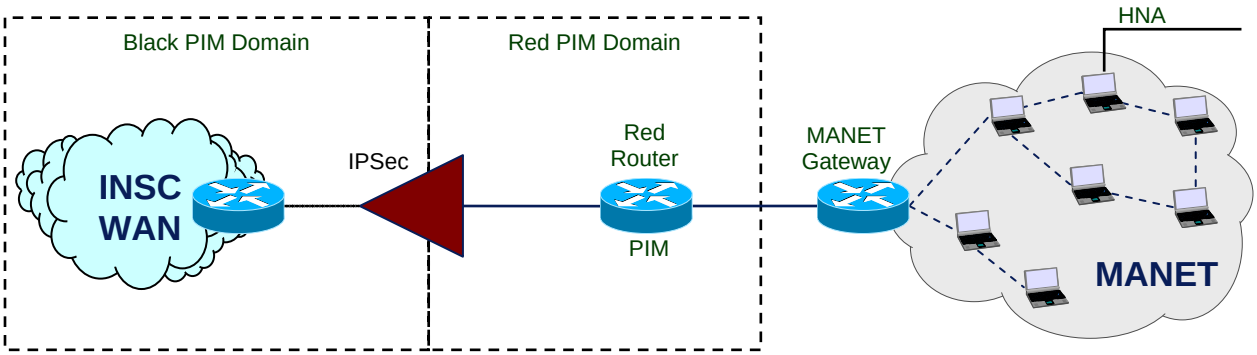

Figure 18: INSC Multicast Network Infrastructure

2.6.1 Group Membership

Before multicast data can get into or out of the MANET, the MANET first needs to join the multicast group. Group membership is done through the use of IPv4 Internet Group Management Protocol (IGMP) or IPv6 Multicast Listener Discovery (MLD) join and leave messages. PIM will take care of group membership inside the PIM domain, but the PIM edge router must be informed of group membership before it will forward data to or from the MANET. This may be accomplished using a static configuration, but that solution requires predetermined groups, and it is inefficient, since multicast data will be forwarded and flooded throughout the MANET, decreasing network capacity whether any nodes are listening to the multicast flows or not. Task 3 members therefore agreed that a dynamic join/leave solution would be best, so static configuration methods were not investigated in detail.

IGMP and MLD are both one-hop protocols, meaning that routers in a multicast chain must not forward IGMP/MLD messages upstream, but must instead proxy, or join/leave *on behalf* of their downstream nodes. The IGMP/MLD proxy concept [42] enables dynamic multicast routing in tree-based network topologies, without needing to run a full multicast routing protocol such as PIM. Unfortunately, the tree topology formed by the MLD proxies must be loop-free, which limits its usefulness inside a MANET.

The MANET gateway, as well as any attached network (HNA) gateway, is capable of proxying IGMP/MLD messages on behalf of the MANET/HNA if it can receive the messages from the end nodes. This functionality can be provided either by the SMF implementation, as is done in the CRC SMF implementation, or through use of the *MLD_Proxy* program [43]. These IGMP/MLD messages are multicast, but they use a link-local address and have a Time To Live (TTL) of 1 due to the one-hop nature of the protocols, so the packets cannot be forwarded by SMF without violating the IP standard. The ideal solution to this problem would be to send MLD messages using a MANET-

local address (with appropriate TTL) so that the packets can be flooded within, but not outside, the MANET. Unfortunately, while the MANET-local address space has been proposed within the IETF, it does not exist at this time. For INSC purposes, we are limited to either violating IP by forwarding the packet inside the MANET without modification of the TTL as the CRC implementation does [44], or simply joining the group at all nodes, since every node will get the traffic from SMF whether it is listening or not.

2.6.2 Forwarding Multicast Packets

Once the MANET has joined the multicast group properly (the PIM router has received the join), through whatever method, multicast packets will begin to flow to the MANET gateway. These packets must then be forwarded onto the MANET interface so that they may be forwarded by SMF. This forwarding may be done either by *MLD_Proxy* or by the SMF implementation. This same functionality should also allow multicast traffic to be forwarded from individual MANET nodes to the PIM router. However, Task 3 members found that PIM was not forwarding these messages into the PIM domain, due to some PIM design assumptions.

PIM routers expect multicast packets to come either from another PIM router or from a machine directly connected to its other interface(s) [45]. Task 3 members attempted to configure their red PIM routers such that the prefix of the MANET-side interface included the MANET's address space. This worked, until the red PIM router was given a unicast route to the MANET address space (so that the MANET nodes could be reached via their unicast addresses). Once this route was added, the PIM router began rejecting packets from the MANET again. The ideal solution to this problem is to simply disable this functionality within PIM, which Task 3 members were unable to do successfully. There is an option to turn off reverse path lookup in IPv4 for Cisco and BSD routers, but this option does not seem to exist in IPv6. Reverse path forwarding should not need to be turned off completely, however – PIM simply needs to ignore the fact that the destination is more than one hop away. This problem also cannot be solved by running PIM on the MANET gateway, as that would only force the problem further down into the MANET, where nodes will again have multiple-hop routes to other MANET nodes. It may be possible to have the MANET gateway send signaling to the PIM router so that it appears to be a PIM router, without actually running the full-blown PIM protocol. This solution needs further investigation to see if it is feasible.

The solution that some Task 3 POs ended up using is to have the MANET gateway overwrite the source address in every multicast packet with its own, or with one valid on the PIM router's local interface. The packet's checksum must also be recalculated using this solution. This functionality is provided by the *MLD_Proxy* program, though it could also be done by the SMF implementation, as the CRC SMF implementation has done. This solution was shown to work, although it unfortunately breaks end-to-end communications because the original source address is lost. A possible alternative to investigate is to encapsulate multicast packets at the MANET gateway, rather than simply overwriting the source address. This extra header would need to be stripped away before the packet would be useful to an application, however.

The *MLD_Proxy* program [43] used by Task 3 members provides a nearly-complete solution for an IPv6 MANET multicast gateway. It takes care of MLD proxying, forwards multicast packets in both directions, and overwrites the source address so that packets sourced in the MANET will be accepted by PIM. It can also be run on nodes which have attached networks, so that attached nodes can send and receive multicast packets. The only problem it does not solve is how to get MLD messages to the gateway from multiple hops away. It should also be noted that this software has some major problems that need to be addressed before it is used in the real world. The code suffers from instability issues, and it does not keep track of which MANET node(s) are joined to a given multicast address, which means it will leave a multicast group whenever any one MANET node leaves the group. Additionally, the software is inefficient, in that it sends a proxy join each time a MANET node joins the network. These issues may be fixed, however, and the complete functionality could also be moved directly into any SMF implementation. It should be noted that the CRC has now fixed these issues and has included this functionality within their SMF implementation (see [44] for details). Further work should be done to investigate the interactions of multicast MANET gateways with various PIM options.

2.7 Black-Side MANET

MANETs were envisioned and investigated within INSC for deployment mainly in the Coalition LAN, that is, on the red (protected) side of an IPSec gateway. When deployed in these areas, link layer security mechanisms are critical for MANET devices. However, there are also deployment scenarios where MANET routing is desirable in the black WAN as well. If these black MANET routing devices are also consumers and producers of data themselves, an appropriate security boundary is required internally at each mobile unit.

Within INSC II, some partners investigated the deployment of MANETs within the black part of the INSC network. The chosen approach was to use IPSec gateways to protect the hosts and networks connected behind the MANET nodes. In cases where the protected hosts and networks are mounted in a fixed fashion on a MANET vehicle or as a Body Area Network on a soldier, their connection can be done in a wired way, avoiding the additional security concerns inherent in wireless networking. An open issue remains regarding whether Layer 3 security provides enough protection for such devices. Link layer security methods may still be desired to provide additional robustness to a variety of threats.

Proof-of-concept field trials have shown MANET successfully working in the WAN for both unicast and multicast traffic using OLSR and SMF.

2.8 MANET Autoconfiguration Work

Autoconfiguration is primarily used to describe the automatic configuration of an IP address for a machine. However, it may also include the configuration of the default gateway and the discovery of network services, such as Domain Name System (DNS),

printers, servers, etc. Task 3 focused on IPv6 autoconfiguration, due to the IPv6 focus of the INSC project.

2.8.1 IP Address Autoconfiguration

An IP address may be manually or automatically configured. In a rapidly-deployed and large tactical MANET, it is desirable that each device's IP address is automatically configured to remove the burden and inflexibility of manual configuration in barracks, where the exact nature of the deployment may not be known (e.g. new nodes could join the network subject to security restrictions) or, worse, configuration in the field.

Two main types of autoconfiguration are available in IPv6. Stateful autoconfiguration, such as Dynamic Host Configuration Protocol (DHCP), requires a server to keep state on its client machines in order to prevent duplicate addresses. The server often assigns the IP address to each client. Stateless autoconfiguration [46] uses a network prefix and the interface's EUI-64 address, which should be unique at least in a controlled military environment, to automatically assign a unique IPv6 address. This method of autoconfiguration does not exist for IPv4.

In IPv6, there are several types of IPv6 addresses. Link-local addresses are valid and unique only on a given link, and are generally assigned via stateless autoconfiguration. Packets sent with a link-local address cannot be forwarded. Global addresses are globally unique and globally routable. Site-local addresses are similar to the IPv4 private address space (10.x.x.x, 192.168.x.x). They are valid and routable within a given "site", but are not globally unique, as other sites will use the same address space. Site-local addresses have been officially deprecated by the IETF, though there are currently proposals to create a similar MANET-local address space for use inside a MANET.

Devices in a single MANET may use a private or local address prefix to (auto)configure an address that is unique within the context of the local MANET. This has the advantage that no coordination is required with external network administration in order to allow devices in the MANET to communicate. However, privately or locally addressed devices may not communicate with devices outside of their local network due to the lack of global routability and uniqueness of the addresses. The requirements for a MANET IP address autoconfiguration protocol are therefore to automatically assign globally unique, globally routable IP addresses to the devices within a MANET. Such techniques exist for fixed networks, including stateless autoconfiguration using Router Advertisements (RADV) and DHCP, but these methods are unable to cope with the multi-hop nature of MANETs.

2.8.1.1 DHCP

DHCP is a stateful autoconfiguration method using a client/server approach. Clients broadcast an address request, and the server replies with an IP address assigned from its pool of available IP addresses. This only works on a one-hop basis, but fortunately, the DHCP specification [47] [48] includes the concept of a DHCP relay to support multiple hop operation. DHCP relay has two modes of operation. In the first, the DHCP

relay hears the client broadcast, and then broadcasts a request on behalf of that node. Once the DHCP server receives the request, it broadcasts a response, which is then relayed back to the client in a similar fashion. This mode of operation is very problematic in a MANET because of loops, and results in a “broadcast storm” with relays endlessly relaying packets for one another. These broadcast packets cannot be forwarded to the DHCP server by a MANET multicast protocol because they have a TTL of one. The second mode of operation is where the DHCP relay forwards the request to the server via a unicast packet. The DHCP server sends the response back to that relay agent via unicast, and the relay broadcasts the response packet directly to the client. This mode of operation requires a MANET unicast protocol such as OLSR to be running on the relay node. This is not a problem, as it allows a MANET to be autoconfigured and built outward from the DHCP server. This has been successfully tested by Task 3 members in IPv4, but could not be tested in IPv6 because no available IPv6 DHCP implementations include a fully functional DHCP relay agent at the time. The only issue with this unicast method is that multiple DHCP relays may hear and relay the request to the server, which will then respond to each relay individually, assigning the same IP address. This is merely a slight inefficiency, however. One open issue with MANET autoconfiguration using DHCP in general is that as a stateful autoconfiguration method, it requires a server, which may not be reachable if a MANET partitions.

2.8.1.2 Stateless Autoconfiguration

Task 3 also investigated stateless autoconfiguration using distributed Router Advertisement (RADV) daemons. This technique requires the gateway device manage a globally unique and globally routable prefix (administered by a global network authority) and to advertise this prefix using RADV. Nodes within one hop of the gateway listen to the prefix advertisements and use that to statelessly configure their address (which is globally routable and globally unique, assuming the EUI-64 identifiers are unique in the local network). Each of those nodes must then start RADV and advertise the same prefix. Neighbors of each of these nodes then go through the same process. In this way, the MANET may be autoconfigured outward starting at the gateway node, and this has been successfully tested by the US. It is also possible to build such a network without using regular router advertisement intervals, as nodes attaching to the MANET will automatically request a prefix via RADV when configured to obtain an IP address statelessly. In this way, prefix advertisement only needs to be done upon request. The disadvantage to this method is that it does require some pre-configuration of the RADV server on each node. The prefix to advertise can be determined from the node’s autoconfigured prefix or from the RADV messages themselves, but settings such as the MANET interface name and advertisement intervals are not as easy to determine, though default settings may work. Open issues with this method include operation with multiple gateways and/or multiple prefixes, as well as scenario-specific issues, such as what to do if a gateway leaves the network (remove the address and stop advertising it, or keep using it to maintain connectivity within the MANET?).

One similar method proposed by IT for statelessly autoconfiguring a MANET does not use the RADV daemon, but instead floods prefix advertisements throughout the MANET. In addition, this solution is able to arbitrate the presence of multiple globally unique prefixes being advertised by multiple gateways. One side-effect of gateway-based IP address autoconfiguration, devices are able to select the gateway that provides them with a global prefix as their default gateway to communicate with external devices. Again, in the presence of multiple gateways, the autoconfiguration protocol must arbitrate which gateway is selected by each device in the MANET.

Using this method, global prefixes are periodically announced by gateways to the MANET using a custom type of OLSR message, defined Prefix Advertisement (PA) messages. Such messages are disseminated to the whole MANET by means of the MPR-based forwarding algorithm in OLSR, but the messages could easily be removed from OLSR completely and forwarded using SMF. Each node associates a validity timer to a received prefix and refreshes it every time a PA message containing the prefix itself is received. If the validity timer expires, the correspondent prefix is considered invalid and deleted. The integration of auto-configuration protocol within OLSR implies that a node needs to participate to routing protocol in order to receive the available global prefixes. Thus, the node must be autoconfigured with a locally-scoped address (e.g. site-local, MANET-local) so that it may participate in OLSR. Once this is done, it will autoconfigure a global address using the global prefix received from the default gateway (which is set through the use of OLSR HNA messages) and advertise that global address in a Multiple Interface Declaration (MID) message. This may all be avoided when using SMF to flood the prefix advertisement, rather than OLSR. However, the use of a locally-scoped address as the primary OLSR address may ease multiple gateway operation.

Each time a node discovers a gateway, it receives the corresponding prefix and builds a global address and inserts it into MID messages. When a node’s default gateway changes, the global address associated to the previous default gateway is removed from the interface, and the global address associated with the new default gateway is configured in its place. When the timer associate to a prefix expires, the correspondent global address is no more inserted into MID messages (Figure 19).

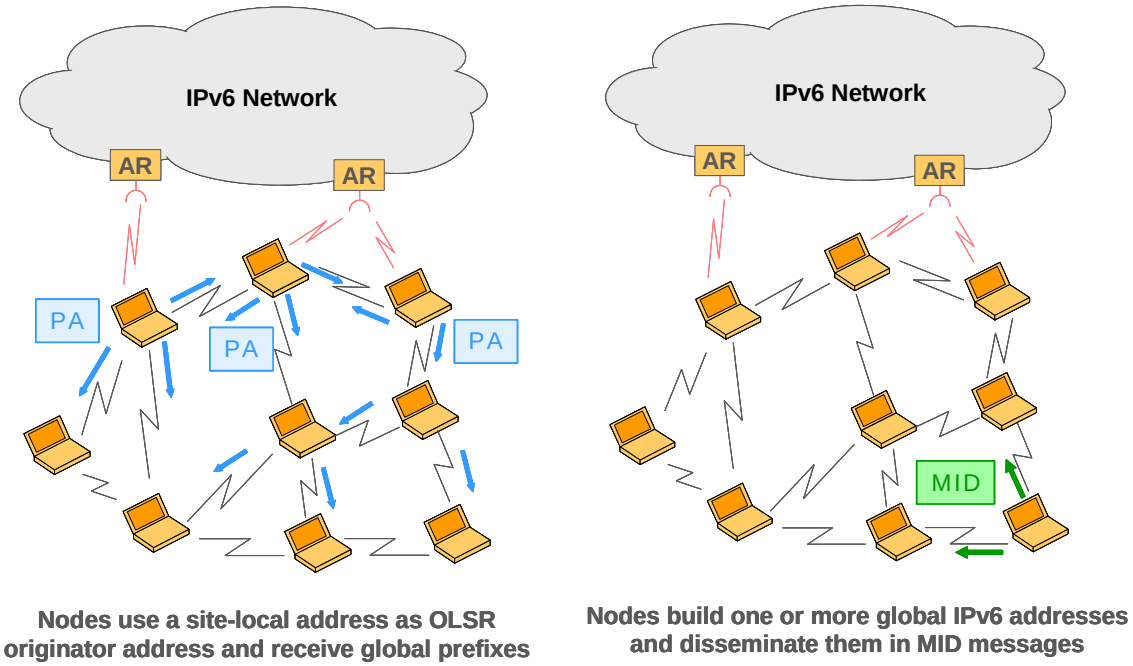

Figure 19: Global address configuration framework

The algorithm of gateway selection for global address configuration aims at optimizing the path followed within the MANET by return downlink traffic incoming from the external network. Indeed, downlink traffic is routed towards the gateway owning the prefix used by node to build source address for uplink data packets. Therefore, by configuring only the global address derived from the default gateway on its interface, a node forces the source address of its uplink data traffic packets and return downlink traffic is consequently delivered to the default gateway and follows the best path within the MANET. While this is more efficient, some sort of hysteresis may be desired to prevent frequent data session interrupts from occurring due to default route changes under mobility. It is also worth noting that several global addresses (associated to different gateways) may also be configured to avoid this problem, but then the downlink data path may be not optimized.

OLSR MID messages announcement and processing is necessary to set up routes towards all the available global addresses. Each node announces all its built global addresses within the MANET, whether they are configured or not. Each node has a route towards each global address of each MANET node and can deliver traffic incoming from the external network to its destination. Such redundancy of routes, coupled with the use of a locally-scoped address to participate to OLSR, is introduced in order to handle the change of the configured global address in an efficient way. Indeed, the delay experienced after the change of the configured global address is ideally reduced to zero since OLSR doesn't have to restart or recalculate routes. The aforementioned changes of the configured global address can happen after several topological events which imply the loss of connectivity towards the default gateway (e.g. partitions, gateway failure or departures) or the change of the default gateway (because a better gateway is available).

This solution has been implemented as an extension to Unik OLSR and was successfully tested. For further details on this solution, please see the IETF draft [49].

The UK also investigated a stateless autoconfiguration solution from the LSIIT Laboratory, called GWINFO [50] (based on [51]). This autoconfiguration method is similar to the IT approach described above, in that it assigns a local prefix to all nodes so that OLSR may be used. However, instead of using a custom OLSR message type, this implementation uses a custom multicast forwarding implementation that relies on the OLSR routing protocol. For multiple gateway operation, the standalone implementation (the OLSR-integrated version could not be compiled) requires the routing protocol used in conjunction with the autoconfiguration protocol to be able to cope with the dynamic change of an IP address. This was tested with NRLOLSR, which does not support this functionality and needed to be restarted to redistribute the new prefix.

2.8.2 Default Gateways and Service Discovery

In addition to configuring IP addresses, it is often useful to configure default gateways and other services such as DNS. In MANETs, default gateway discovery is often taken care of by the routing protocol. Proactive MANET protocols such as OLSR and MANET-OSPF have methods for advertising networks attached to MANET nodes, and these methods can also be used to advertise a default network route. Default gateway discovery using reactive MANET protocols such as AODV is generally more difficult. Since routes are discovered “on demand,” there is no easy way to determine if a given route is a “default” route, or if there is a more specific route in the network for that packet. This is an area of ongoing investigation within the IETF.

In addition to assigning IP addresses, DHCP has options which allow it to assign a default gateway and set up other services such as DNS. DHCP is also extensible, allowing any sort of service discovery to be done using DHCP. It is worth noting that DHCP can be run in a mode in which it does not assign an IP address, but still hands out desired service discovery and/or default gateway information.

2.8.3 Distributed MANET DNS (DMDNS)

The conventional Domain Name System (DNS) is structured as a set of servers holding sections (or copies of sections) of a database of logical name to IP address mappings for devices and services in a managed namespace. This mapping makes it easier for human operators to use services and communicate with remote devices through the use of convenient human-readable names. DNS relies on the manual designation and administration of DNS servers and while Dynamic DNS (DDNS) can alleviate some of the effort involved, manual administration is still required. In addition, DDNS is by no means a globally-deployed standard. In contrast, the UK has developed the Distributed MANET DNS (DMDNS) protocol as a wholly autoconfigured name resolution service for ad-hoc, military networks where the skills, time and planning required to administer conventional DNS are undesirable.

DMDNS makes use of the unique role names (e.g. capt.aplat.acoy.3bde.uk) assigned to military users. These role names (along with additional information) are stored on security tokens specific to each user. The token is used to authenticate the user with a military network when inserted into a computing device attached to the network. DMDNS makes use of this information by automatically reading the unique role name from a security token and forming a DNS name-to-address mapping, or Resource Record (RR), using the name and an interface's IP address on the device into which the token has been inserted. This is an automatic process, and the movement of a user between devices will be reflected by the updating of the RR on the new device. As each active device in the network will autoconfigure its own RR, it can be seen that the conventional centralized DNS database is now distributed across all of the active devices. To access the database, a modified client DNS resolver library is required that looks similar to a conventional DNS resolver, but with additional functionality. The current prototype requires applications to be slightly modified to use this new function but it should be possible to transparently redirect existing application binaries to invoke the new function.

In the intended context of a MANET, DMDNS requires the use of an efficient transport to disseminate resolver requests to every node in the MANET (as each node holds its own part of the DMDNS database). The ideal solution is to use one of the simple MANET multicast forwarding protocols also studied in INSCII Task 3, such as SMF. Thus, all DMDNS resolver requests are multicast to all members of the MANET and the device with the corresponding RR provides its IP address as a unicast reply to the originating application, which can then proceed as normal (see Figure 20).

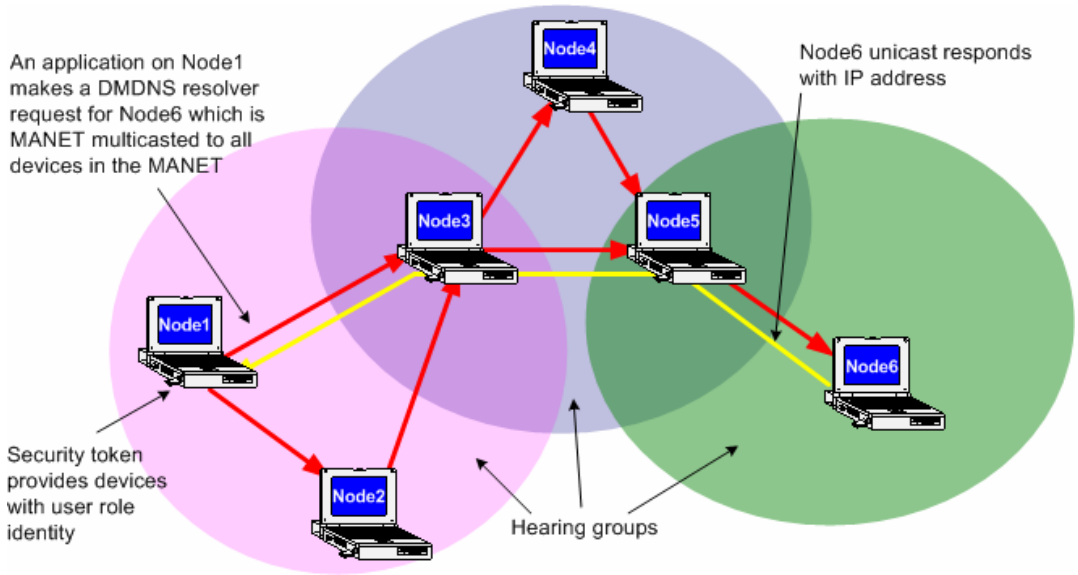

Figure 20: The DMDNS Process in Action

By virtue of being a distributed algorithm, DMDNS also exhibits strong properties of resilience. For instance, if there are devices located in part of a network that has become fragmented from a standard DNS server, then any DNS resolution requests they make will fail and the devices will be without DNS services, and unable to locate

other users by role, even in their own fragment. DMDNS is able to continue to resolve roles in the local fragment, which, given the nature of the network fragmentation, will be critical for allowing users in the fragment to continue operating as a coherent fighting force. In addition, a special DMDNS request asking for all reachable devices to return their name-to-address mapping could be implemented that provides details of all users still active in the local fragment.

One outstanding issue of DMDNS which still requires further investigation is the interaction of DMDNS with conventional DNS as used in other (e.g. fixed) parts of the military network. A gateway DMDNS to DNS proxy device is the most likely solution.

The UK has implemented a prototype DMDNS implementation in IPv4. This includes a replacement DNS resolver library and a resolver daemon running on each device. In addition, an FTP application has been modified to make use of DMDNS and a UDP messaging application will be modified shortly for use in the UK National demonstration. An initial performance evaluation of the prototype DMDNS implementation has been conducted on the UK Large Network Emulator (LNE) alongside conventional DNS using a 20 node mesh MANET. The performance results showed that overall, DMDNS exhibited higher network overheads than DNS, since each resolution request is forwarded to every device in the network, rather than to just the DNS server. However, the resolution times of DMDNS were better than for DNS. This was attributed to the heavyweight nature of the DNS protocol, which generates lots of packets between the client resolver and the DNS server. This makes that route susceptible to collisions, at which point DNS will wait for a timeout before retrying. In contrast, DMDNS is extremely lightweight, as it does not implement the full DNS protocol specification. This is a consequence of DMDNS's goal of supporting smaller stub tactical MANETs as opposed to the requirement of DNS to scale to very large hierarchical networks.

3 Edge Mobility Technology

Edge mobility focuses on mobile users, systems, or even entire mobile networks that are capable of macro-mobility, moving across routing borders and within a larger wide area network (WAN). The main edge mobility technologies that were investigated by Task 3 are Mobile IPv6 (MIPv6) [52], designed to support individual roaming mobile hosts, and Network Mobility (NEMO) [53], designed to support roaming aggregate networks. Both technologies require a supporting home agent (HA). The HA acts as an anchor point for roaming nodes or networks within a larger network, under the assumption that these nodes wish to retain their home-based associations and addresses. This is often useful if the roaming node or network has a server functionality that needs to maintain dynamic reachability via its old "home" address, or if there is a need to maintain existing connections while undergoing roaming conditions.

At a basic level, this broader type of mobility function is not always required since other methods including Dynamic Host Configuration Protocol (DHCP), peer-to-peer middleware, and dynamic Domain Name System (DDNS) can allow for various degrees of edge system mobility support. A simple network client node (e.g. bursty web client) can simply move to a new area, obtain an address using DHCP or some other method

(e.g. stateless autoconfiguration) and continue functioning as normal. More enhanced alternatives would include the additional use of dynamic DNS or possibly P2P middleware to update and register mobility information to allow clients to initiate communications with a mobile server, but existing sessions would need to be restarted. While these possible architectural alternatives should be considered in a broader context, Task 3 focused its examination and demonstration efforts around MIPv6 and NEMO technology and the relevance of this technology within a coalition battlespace application.

3.1 Mobile IPv6 Autoconfiguration

Much work was done in INSC Phase I on Mobile IPv6. For details on that work, see the INSC Phase I Task 6 Final Report [2]. Mobile IPv6 work in INSC Phase II focused on the area of autoconfiguration.

Mobile IPv6 requires that Mobile Nodes (MNs) and Home Agents (HAs) share a set of configuration parameters. The MN must know its home address, the Home Agent address, and the cryptographic material needed to protect MIPv6 signaling (e.g. shared keys or certificates to setup an IPSec security association). One approach to obtaining this information is to statically provision the necessary configuration parameters on the MNs and HAs. This solution is sub-optimal from a deployment perspective, especially in large networks with a lot of users. In addition, the extensive use of manual and static configurations limits the flexibility and reliability of the system, in that it is not possible to dynamically assign the HA when the user enters the network, which would help to optimize performance and resource utilization (e.g. assignment of the HA closest to the MN's point of attachment). This is generally referred to as the Mobile IPv6 bootstrapping problem. Based on different scenarios (i.e. integrated and split), the IETF is completing the development of two solutions [54] [55] that differ on the approach used by the MN to obtain the HA address (i.e., discovery through DNS or assignment through DHCP).

During INSC Phase II, IT developed an alternative solution to the MIPv6 bootstrapping problem that, compared to those being devised by the IETF, has the advantage of enabling better control of mobility service and removing the need for a full Extensible Authentication Protocol (EAP) between the MN and HA for MIPv6 authorization. The proposed mechanism is subject of an Internet Draft [56] submitted within the MIP6 working group of the IETF.

The basic idea behind the solution proposed by IT is to perform Mobile IPv6 bootstrapping during the authentication procedure undertaken by the Mobile Node to gain network access. In particular, the solution defines a method to:

- Explicitly authorize the use of Mobile IPv6 based on the service profile of the user, its position within the network, etc.
- dynamically allocate a Home Agent to the Mobile Node
- Dynamically configure Mobile IPv6 start-up parameters (i.e. MIPv6 bootstrapping) on the Mobile Node. These parameters include the Home Address and the cryptographic material needed to set-up the IPSec Security

Association used to protect Mobile IPv6 signaling (i.e. Binding Updates and Binding Acknowledgements)

Figure 21 shows the overall architecture of the MIPv6 bootstrapping solution. The central element of the architecture is the Authentication, Authorization and Accounting (AAA) server on the home domain, which interacts with both the MN and the selected HA to perform service authorization and configuration. The solution is applicable to any access network relying on EAP for user authentication and works with all EAP methods supporting the exchange of general purpose information elements, in any form (e.g. TLVs or AVPs), between EAP peers. Exploiting this capability, the MN and home AAA server can piggyback Mobile IPv6 negotiation messages within the same EAP conversation used to carry out user authentication.

This kind of operation is already supported by several tunneled (e.g. PEAPv2) and non-tunneled (e.g. EAP-IKEv2) EAP methods, that also include native support for encryption, authentication and integrity protection of exchanged configuration information (e.g. HA address).

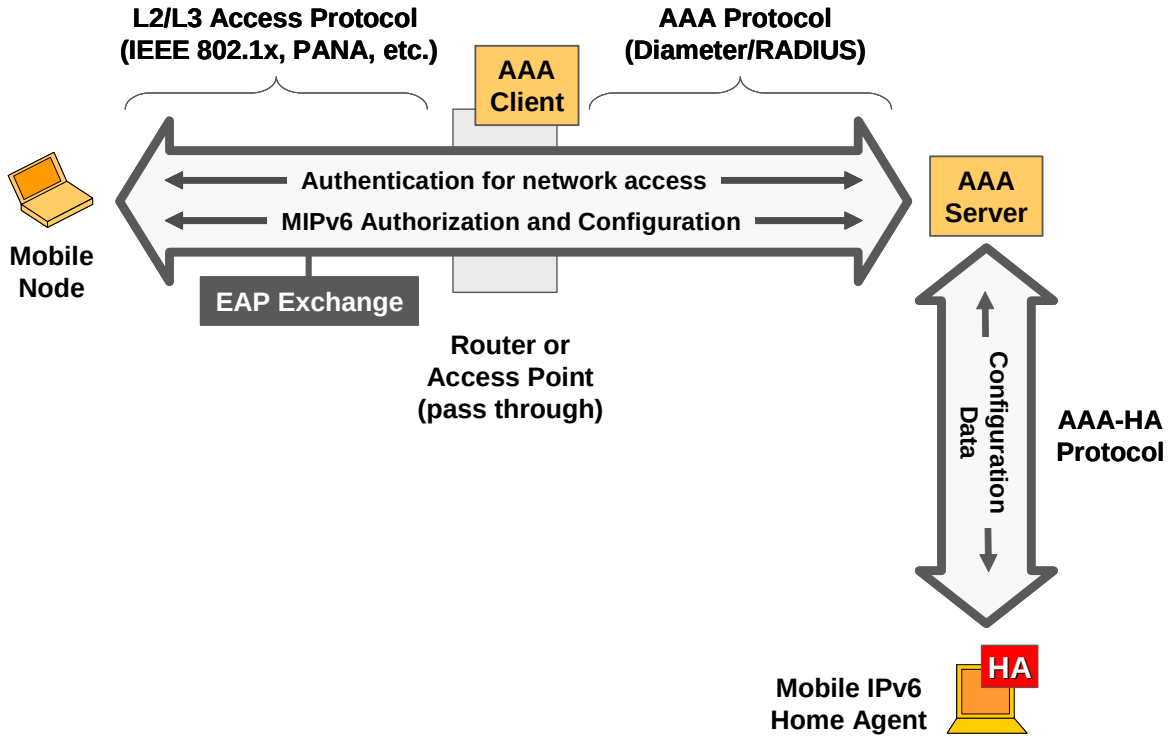

Figure 21: Mobile IPv6 bootstrapping based on EAP

The proposed architecture allows the home domain to maintain a centralized management (on the AAA server) of the user profiles and the authentication, authorization and accounting procedures for any type of service, including Mobile IPv6. Moreover, the solution has the following advantages:

- improves the reliability and performance of the Mobile IPv6 protocol, in that the HA to be dynamically assigned to the MN can be freely chosen among those that

are closest to the user's point of attachment, thus optimizing network usage and reducing the transfer delay for data traffic in bi-directional tunneling

- Can be deployed, or extended with new features, without having to update the access equipment and the AAA protocols in use. Only minor changes in the AAA servers, the Home Agents and the mobile terminals are required, in that the AAA client does not play any active role in MIPv6 negotiation (i.e. it is a pass-through for EAP signaling). This reduces the deployment costs and makes the solution easy to use even when a Mobile Node is roaming with an administrative domain different from its own
- Allows the usage of any AAA protocol supporting the transport of EAP messages for the communication between the AAA client and server (i.e. not just Diameter, but also RADIUS). This significantly simplifies the deployment of MIPv6 in existing communication networks, where support for Diameter protocol in access equipment is not so extensive
- Allows the home domain to dynamically choose the authentication method for Internet Key Exchange (IKE) bootstrapping and to automatically distribute the pre-shared key eventually needed. In this way the pre-shared key must not be preconfigured and can be frequently changed increasing resistance to attacks. In the case of an EAP method providing dynamic generation of keying material, the pre-shared key can be derived from EAP hierarchy, avoiding the need to explicitly send it to the MN.

As a whole, the solution adds a maximum of 2 Round-Trip Times (RTTs) to the EAP conversation carried out by the MN to authenticate itself and gain network access. The number of extra RTTs can be reduced if the employed EAP method has the capability of transporting MIPv6 negotiation TLVs (or AVPs) together with authentication data. Nonetheless, it should be noted that the full negotiation procedure can be undertaken by the MN only during its initial bootstrapping, and therefore the performance requirements are not so strict.

The overall architecture of the implementation carried out by TI is depicted in Figure 22.

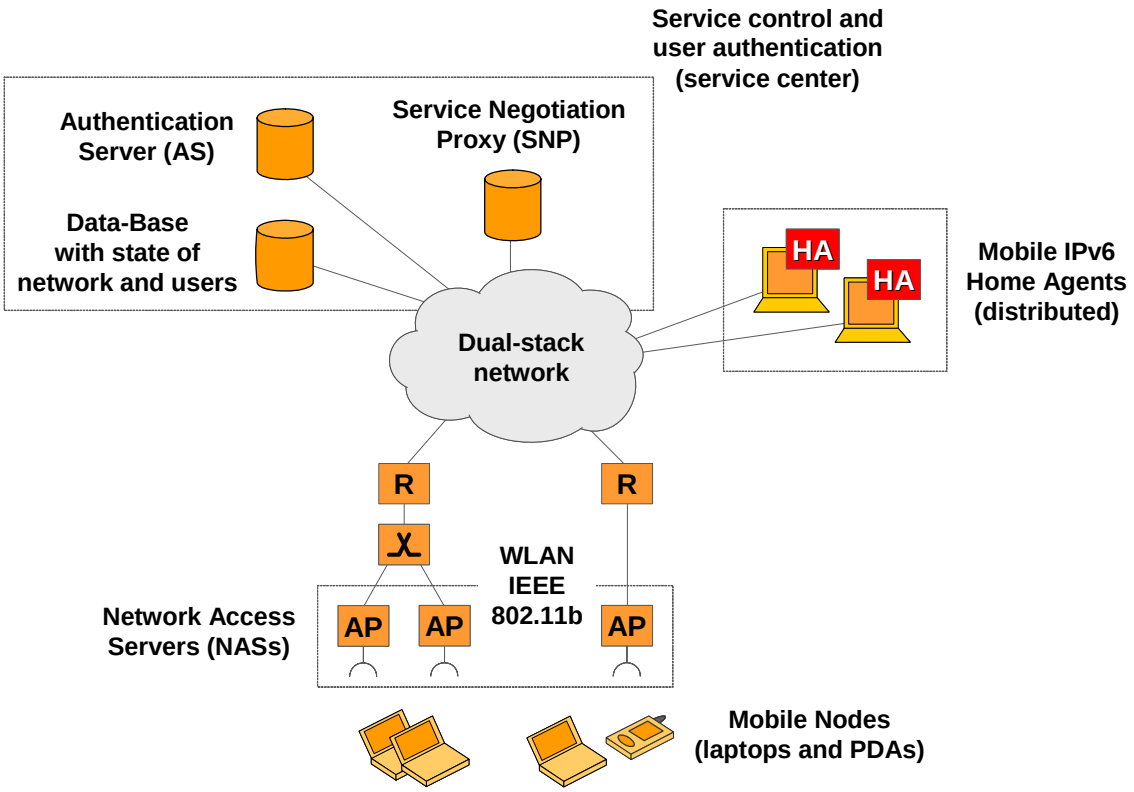

Figure 22: Architecture of TI platform for dynamic MIPv6 authorization and configuration

The access infrastructure is a Wireless LAN conformant to the IEEE 802.11b standard. In order to gain access to the network, the WLAN terminals are required to undergo an authentication phase based on the Extensible Authentication Protocol (EAP), which is transported over IEEE 802.1X on the radio interface.

EAP is an authentication framework which supports multiple authentication methods. The EAP method that has been implemented within the TI prototype is Protected Extensible Authentication Protocol version 2 (PEAPv2), which is a tunneled EAP method. In PEAPv2, the conversation between the terminal (i.e. EAP peer) and the AAA server (i.e. EAP backend authentication server) is encrypted, authenticated, integrity and replay protected within a TLS channel.

PEAPv2 is comprised of a two-part conversation. In Part 1, a TLS session is negotiated, with server authenticating to the client and optionally the client to the server. The negotiated key is then used to encrypt the rest of the conversation. In Part 2, within the Transmission Layer Security (TLS) session, zero or more inner EAP methods are carried out. Part 2 completes with a success/failure indication protected by the TLS session or a protected error. In Part 2, the terminal and the AAA server of the home domain can also exchange a set of arbitrary parameters in the form of TLVs (Type Length Values). Therefore, PEAPv2 is suitable for implementing the Mobile IPv6 negotiation procedure previously described.

As a whole, the network elements that build the TI platform are the following:

- Terminals (or Mobile Nodes): laptops or PDAs, equipped with a Wireless LAN NIC conformant to the IEEE 802.11b standard. Each terminal supports Mobile IPv6 and plays the role of IEEE 802.1X supplicant to perform the authentication procedure required to gain network access. The software client implementing the IEEE 802.1X supplicant, and the employed EAP methods (i.e. PEAPv2 and MS-CHAPv2), has been extended to support dynamic Mobile IPv6 authorization and configuration.
- Wireless LAN Access Points (APs): standard IEEE 802.11b APs playing the role of IEEE 802.1X authenticators and AAA clients. The APs are the Network Access Servers (NASs) responsible for checking the user credentials, through the AAA infrastructure, and enforcing the correspondent authorization policies.
- routers: standard IPv4/IPv6 routers
- Service Negotiation Proxy (SNP): AAA server working as EAP backend authentication server for PEAPv2 (i.e. outer EAP method). SNP works as AAA proxy for the inner EAP method and interacts with the MN and the HA to control all the phases of the Mobile IPv6 authorization and configuration procedure.
- Authentication Server: AAA server working as EAP backend authentication server for the inner EAP method (i.e. MS-CHAPv2)
- Home Agents (HAs): standard Mobile IPv6 HAs extended with the capability to interact with the SNP to achieve dynamic Mobile IPv6 authorization and configuration
- Database: MySQL database where all the service profiles, and the current status of network and users, are stored.

The SNP and Authentication Server can also be implemented on the same machine. They have been kept functionally separated to increase the flexibility of the platform. The interface between SNP and Authentication Server is a standard RADIUS interface. SNP is the central element of the architecture. As part of the Mobile IPv6 bootstrap phase, the Service Negotiation Proxy (SNP) is responsible for choosing the Home Agent that has to be allocated to the Mobile Node (MN). This HA selection process has the objective of identifying, among the available HAs, the one that is best suited for serving the MN, keeping into account performance parameters like the distance in terms of network hops, the current load (e.g. number of registered users, amount of traffic in bi-directional tunneling) and the supported features.

In order to identify the HA that is closest to the current point of attachment of the MN, the access network is divided into different zones, each one including multiple APs and one or more preferred Home Agents. The zone planning is carried out by the network administrator and the resulting zone configuration is permanently stored in the network topology database.

As an example of a concrete deployment of this solution within the INSC Phase II architecture, Figure 23 shows the test-bed configuration that has been foreseen for testing the MIPv6 bootstrapping solution in the IT IPv6 MoD network.

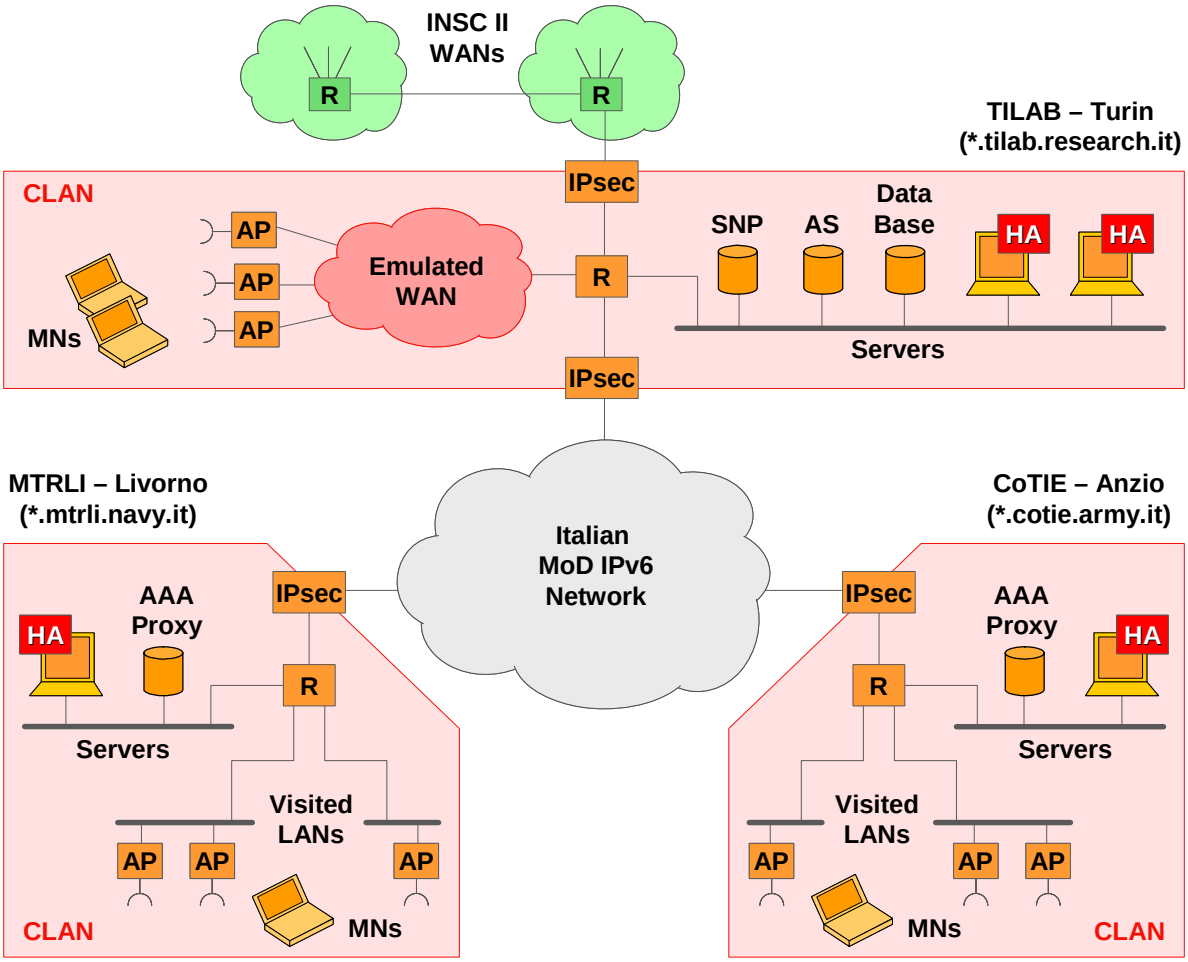

Figure 23: An example of deployment scenario based on IT test-bed configuration

Coherently with the current INSC Phase II assumptions, all the mobility management and AAA functions have been positioned in the protected network (i.e. within the Coalition LANs realized behind the IPSec gateways).

The Coalition LAN located at TILAB (IT) hosts the servers responsible for controlling the Mobile IPv6 service within the whole Italian protected domain. These servers include the Service Negotiation Proxy (SNP), the Authentication Server and the database.

All the users are registered in the database located at TILAB, which is consulted by both SNP and Authentication Server to take all the authorization decisions. Each Coalition LAN is assigned to a different zone identifier within the network topology database located at TILAB (see section 4.3.3). This information is used by the Service Negotiation Proxy (SNP) in the HA selection algorithm, in order to guarantee that any user switching on its mobile terminal within a certain CLAN gets, whenever available, a local HA, unless it has reached its maximum load level.

This configuration can be replicated in operational scenarios involving a central CLAN hosting a command and control centre and multiple CLANs with mobility needs (e.g. including moving soldiers and vehicles) distributed over the territory.

3.2 NEMO Technology

Mobile IPv6 was the focus of edge mobility work in INSC Phase I. During INSC Phase II, this focus shifted to Network Mobility (NEMO), an open standard being developed within the IETF NEMO Working Group. NEMO technology is aimed at finding solutions to manage the mobility of an entire network, which changes, as a unit, its point of attachment to the WAN infrastructure and thus its reachability in the network topology. The mobile network, which is assumed to be a leaf network (i.e., not carrying transit traffic), includes one or more Mobile Routers (MRs) which connect it to the WAN. Another basic assumption is that none of the Local Fixed Nodes (LFNs) of the mobile network have to be aware of the network's mobility and movements, therefore, must be managed transparently with respect to them. A graphic representation of a typical NEMO scenario is shown in Figure 24. The Mobile Router (MR) connects the mobile network to Access Routers (ARs) in various Foreign Networks, which serve as points of attachment to the WAN or Internet. The Home Agent (HA) on the Home Network is used to maintain reachability to the mobile network.

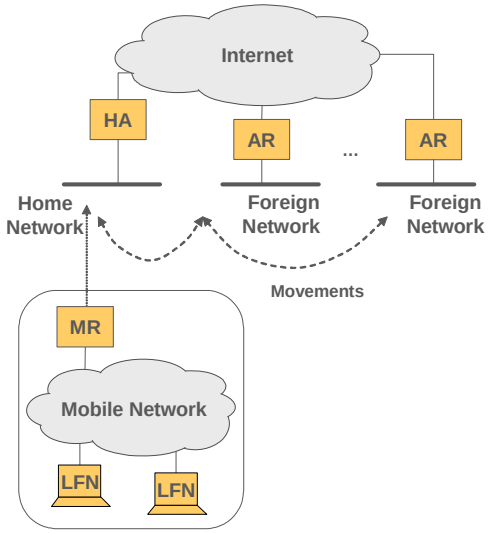

Figure 24: Typical NEMO scenario

The NEMO WG has adopted a stepwise approach by standardizing some basic support mechanisms based on the bi-directional tunneling approach, and at the same time studying the possible approaches and issues with providing more optimized routing solutions. The basic approach is described in the NEMO Basic Support RFC [53], which builds on the Mobile IPv6 protocol. The solution suggests that each Mobile Router establishes a bi-directional tunnel with a Home Agent in order to preserve session continuity while the network moves around. The Mobile Router acquires a Care-of Address (CoA) from its point of attachment, just as is done by MIPv6 Mobile Nodes (MNs), and updates the tunnel in charge of carrying all the traffic flowing between the nodes of the mobile network and their respective correspondents. The extensions to Mobile IPv6 are backward compatible in the sense that NEMO-compliant Home Agents and Mobile Routers are supersets of functionalities of their MIPv6 counterparts. A HA can distinguish a MR from a simple MIPv6 MN by the fact that the MR must set the "R flag" [53] in the Binding Updates it sends.

In order to properly set up the forwarding, a NEMO Home Agent must know which network prefixes are served by a MR. To obtain this information, the RFC defines an ad-hoc mechanism (*explicit mode*) and suggests two other options:

- MR includes the prefix information in the Binding Updates by means of a new Mobility Header option (Mobile Network Prefix Option). This method, called **explicit mode**, can be considered a sort of unidirectional routing protocol between MR and HA.
- HA uses an unspecified custom method to learn the mobile network prefixes, e.g. static configuration of routes. This solution is called **implicit mode**.
- MR and HA run a standard routing protocol on the virtual link represented by the bi-directional tunnel. Support for this method is optional and not fully covered by the current specifications.

When a packet originated in the mobile network reaches the MR, it is encapsulated and sent to the Home Agent (reverse-tunneling), which, after decapsulation, forwards the packet using its routing table. Vice-versa, when the HA receives a packet whose destination belongs to the set of mobile prefixes served by a Mobile Router, it encapsulates the packet with the MR CoA as the destination address. The MR, upon receipt of the packet, decapsulates and forwards it through the interface towards which the prefix is known to be reachable. The tunneling technique in either case is IP-in-IP. It should be noted that the routing infrastructure forwards packets for the mobile network toward the Home Agent or, at least, toward the defended MR Home Address. However, the method used to announce the mobile network prefixes to the routing infrastructure is considered out of scope by the RFC.

The NEMO approach to network mobility allows for the nesting of such networks, where a MR is connected to a mobile network served by another MR, since each MR will appear to its point of attachment as a single node. The current method for supporting this functionality adds extra protocol overhead due to multiple levels of packet encapsulation.

3.3 NEMO Testing Framework

The main Task 3 POs involved in NEMO investigation were IT, GE and FR. Each PO set up a local testbed, in which they carried out functional testing, as well as some limited performance testing. These local tests focused mainly on gaining experience with the reliability, stability and performance of currently-available NEMO implementations. Furthermore, to assess the suitability of NEMO in military environments, real-world field tests involving network mobility scenarios have been carried out.

The main aim of the testing done by Task 3 was to verify the functionality of currently-available NEMO implementations (NEPL for Linux [57] and experimental Cisco IOS versions), and a more comprehensive list of objectives may be considered the following:

- Acquire know-how for installing and configuring devices
- Verify Cisco/Linux interoperability
- Report bugs
- Point out possible protocol weaknesses
- Estimate the handoff latency

The protocol behavior of NEMO has been tested while moving a Mobile Router between its home link and different visited networks. MIPv6/NEMO functionality such as Home Registration, DHAAD (Dynamic Home Agent Address Discovery) and explicit mode were tested while verifying the session continuity of active communications. Both functional and performance tests were done in a localized fashion.

3.3.1 Testbed Infrastructure

The basic infrastructure used to perform testing of NEMO is shown in Figure 25. The platform, placed within a single INSC Coalition LAN (CLAN), includes the following main components:

- one Mobile Router (MR) serving a mobile network including at least one Local Fixed Node (LFN), e.g. Linux PC
- one home network including an IPv6 router working as NEMO/MIPv6 Home Agent
- one Correspondent Node (CN), e.g. a Linux PC
- at least two foreign networks to which the MR may roam

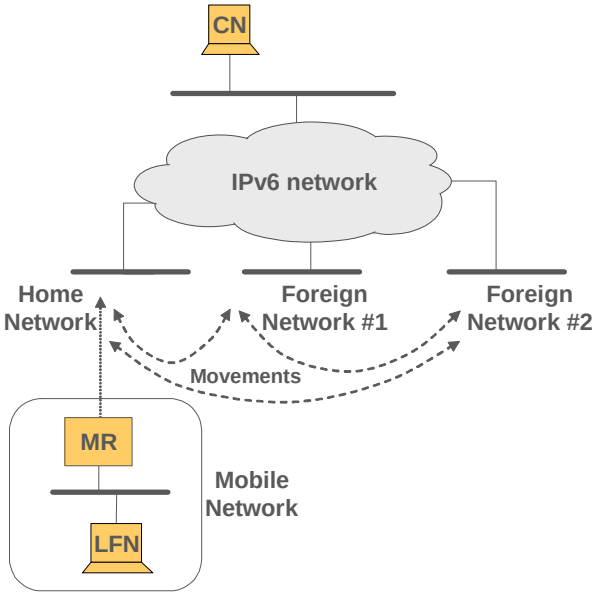

Figure 25: Basic testbed infrastructure

Testing was performed by moving the MR from one subnet to the other (e.g. from the home network to one of the foreign networks and among different foreign networks) while a LFN was communicating with the CN. The movements of MR can be performed manually by disconnecting and reconnecting a cable, but mobility emulation is necessary to carry out performance tests in a repeatable and controlled way. Additionally, it is helpful for functional tests, in that it eases the control of MR mobility. Two different approaches for performing mobility emulation were used by T3 members: the use of a layer 2 switch with programmable VLAN configuration, and the use of a WLAN with tunable SSIDs.

3.3.2 Programmable Switch Emulation

An effective way to emulate terminal mobility within an IPv6 network is to use a programmable Ethernet or Fast Ethernet switch supporting dynamic configuration of Virtual LANs (VLANs). The network infrastructure that can be used for this purpose is depicted in Figure 26.

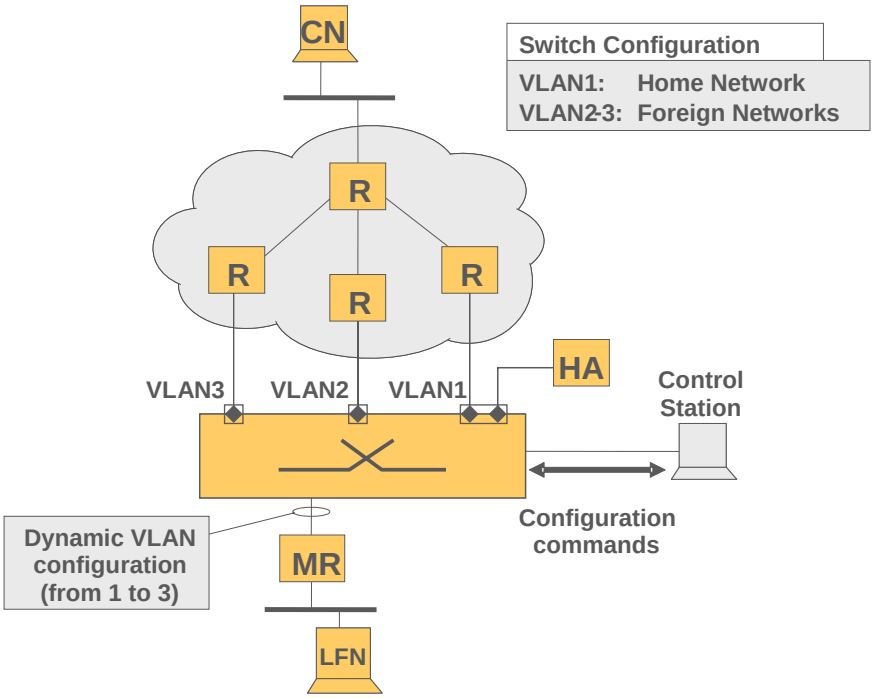

Figure 26: Mobility emulation based on a programmable switch

The IPv6 subnets to which the MR is scheduled to roam (i.e., the home network and all the foreign networks) must be implemented as separate VLANs on the programmable switch, each associated with a well known VLAN identifier (normally a number). MR movements can be forced simply by changing the VLAN identifier associated to the port to which the MR is connected. The MR may be continuously moved among subnets according to a deterministic and repeatable schedule (e.g., cyclic movements among two subnets at a fixed frequency), or following random/statistical mobility patterns.

The layer 2 switch to be used for this purpose may be any Ethernet switch supporting VLANs, such as a Cisco Catalyst. The commands necessary to dynamically adjust

VLAN configuration on the switch may be issued by a control station using communication mechanisms like RSH, telnet or SNMP.

The fundamental characteristic of this emulation approach is that the MR is able to communicate on the new link as soon as the correspondent VLAN reconfiguration command is issued by the control station. There are no relevant extra delays due to the management of layer 2 handover, such as the re-association latency of IEEE 802.11 WLANs, which can be several hundred milliseconds and usually varies with the vendor and the particular configuration of the network. The handoff latency that can be measured when using a programmable switch to control terminal mobility is therefore always lower than in a real system, in that all the MAC layer effects typical of most radio links are completely hidden by the emulation platform. Instead, the performances are affected only by the efficiency of the layer 3 mobility management procedures (i.e., the NEMO/MIPv6 protocols).

3.3.3 Tunable WLAN Emulation

Another way to emulate network mobility within an IPv6 network is to use a tunable WLAN. Instead of implementing the home and foreign networks as separate VLANs on a programmable switch, each of those subnets is physically realized by a separate WLAN access point, and the MR really roams between separate physical subnets. The network infrastructure that can be used for this purpose is depicted in Figure 27.

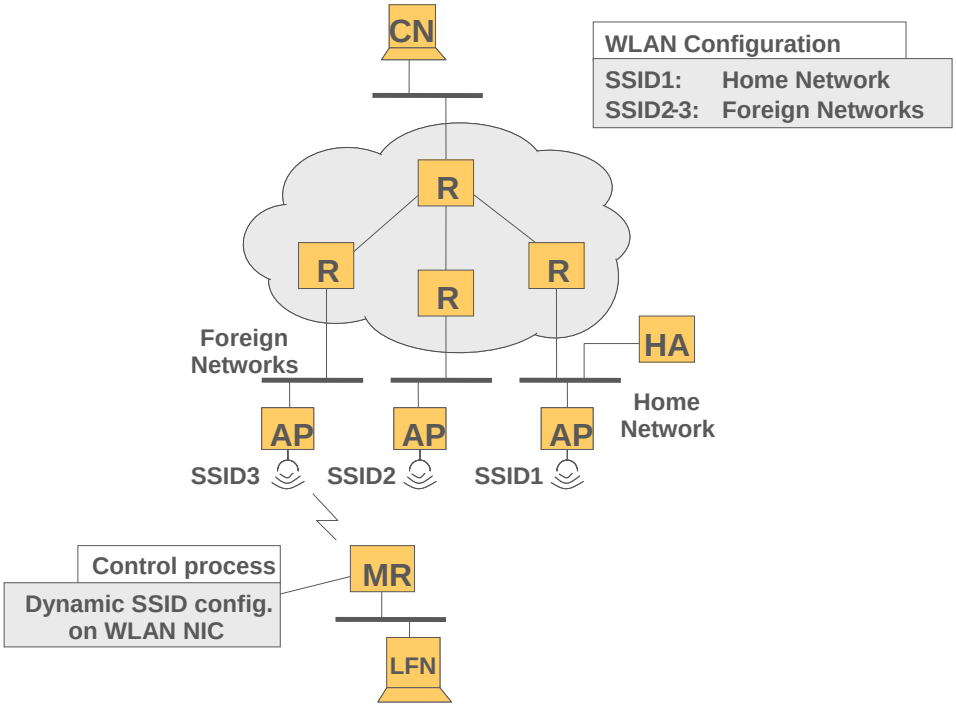

Figure 27: Mobility emulation based on a tunable WLAN

In order to achieve the roaming of the MR without manual intervention, a script running on the MR can automatically reconfigure its wireless settings. For this purpose, each of the WLAN access points is assigned a different SSID, and the MR will only have a

connection to the WLAN corresponding to the SSID it has currently configured. The script will now periodically reconfigure the SSID set on the MR's WLAN card, and thereby automatically trigger its roaming between these different WLAN subnets.

The main difference in using a tunable WLAN for mobility emulation is that there is an added delay due to the link layer association to the WLAN access point, which can be very high (e.g. several hundred milliseconds. Due to this delay, the handover will not be as fast and smooth as using a programmable switch, but for functional NEMO testing, this limitation does not matter.

3.3.4 Italian Testbed Description

The real deployment in the Italian testbed of the reference scenario depicted in Figure 25 is shown in Figure 28, where the entire IPv6 network consists of only one interconnecting router (Cisco 7505). The Correspondent Node and the LFN (Local Fixed Node) were standard Linux PCs, while two Cisco 2600s were employed as access routers in the foreign networks. As active NEMO nodes, the following devices were used (the two MRs were used alternately in the tests):

- **HA:** Cisco 3640; IOS image C3640-IS-M, experimental version 12.4 (20050620:185227) [sgundave-nemocflow 252]
- **MR (1):** Cisco 7513; IOS image rsp-isv-mz.nemo.002, experimental version 12.3 (20050112:000451) [sgundave-kidpaddle.END_OF_TWARWICK_GEO_PI6.9072.sync 145]
- **MR (2):** PC; Linux Mandrake 10.1, MIPL 2 [58], NEPL 0.1 patch

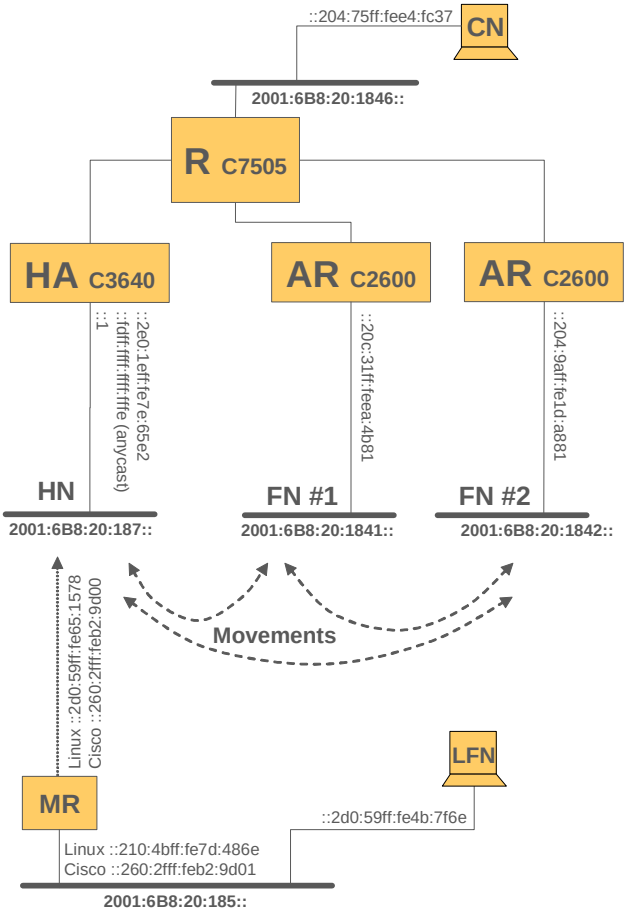

Figure 28: Italian testbed actual deployment

Preliminary tests revealed a major issue with the Cisco 75xx platform: enabling the HA functionality jeopardized the forwarding capability of the router. Packets, including those not related to NEMO, were forwarded through the correct interface, but used an incorrect next-hop MAC address. As a workaround, this platform was relegated to the role of MR. The Linux platform was not used as a HA in the tests.

MR handovers were emulated by implementing each access subnet as a separate VLAN on a programmable switch and changing the VLAN associated with the MR egress interface port (see Figure 29).

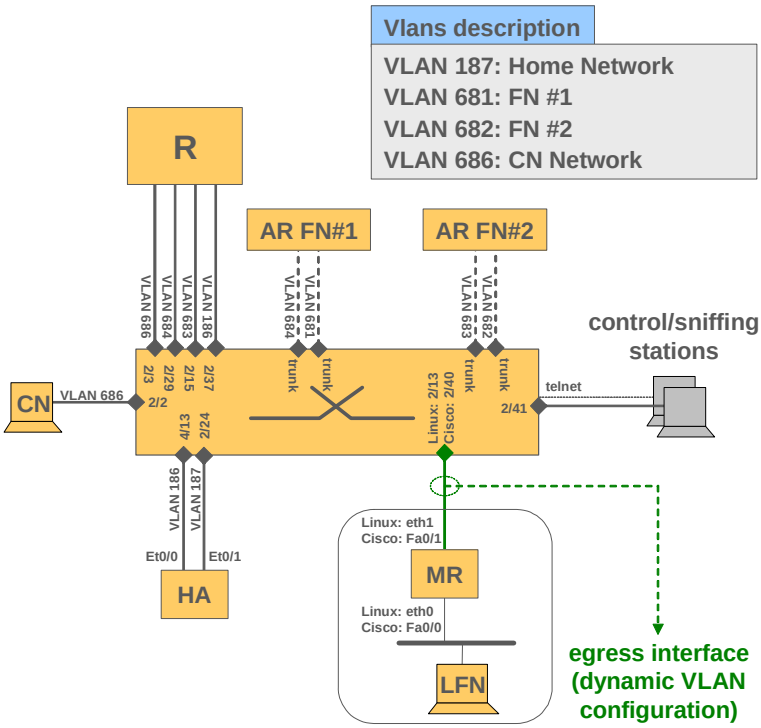

Figure 29: Italian emulation testbed layout

In order to analyze data and signaling traffic flowing through the egress interface of the Cisco MR, that same traffic was mirrored on another port where a sniffing station was connected. Finally, in order for movement detection to work with acceptable performance, all the access routers located in the home and foreign networks were configured to send unsolicited multicast router advertisements at a rate of 500ms. A bug was encountered using the mirror feature: multicast packets generated by the MR (e.g. Neighbor Solicitations for DAD), that is multicast packets entering the monitored port, were mirrored twice on the monitor port. Those packets were manually removed in the textual dumps showed in next sections. The switch is a Cisco 6506 with CatOS 6.1(1a).

3.3.5 German Testbed Description

The setup of the German NEMO testbed, which was used to test only the open-source Linux NEMO implementation, is illustrated in Figure 30. The HA, CN, and the router connecting the home and foreign networks are all Linux PCs with wired Ethernet interfaces. The Mobile Routers MR1 and MR2 are Linux PCs with WLAN egress interfaces and wired Ethernet ingress interfaces. The WLAN access points are Orinoco AP-1000 units.

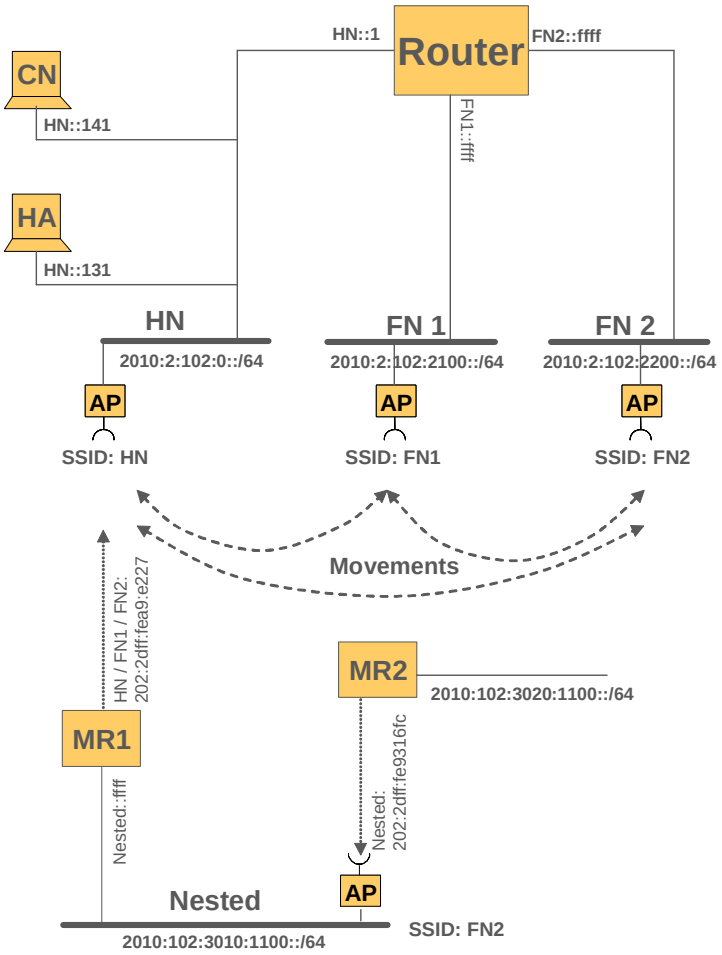

Figure 30: German NEMO testbed

The main test goal with the German testbed was the execution of functional tests with the Linux-based NEMO implementation. For analysis purposes, the control message exchanges between the various components of the testbed were monitored using Ethereal on the home and foreign networks. Furthermore, for easily executing handoffs mainly of MR1 between the home and foreign networks, tunable WLAN emulation was used.

3.3.6 French Testbed Description

The global FR mobility platform is illustrated in Figure 31. The platform is composed of two zones for each environment test. The left zone is for Cisco testing, the right is for NEPL testing. A third zone (Foreign Network) has been created in order to do interoperability tests between Cisco and Linux devices.

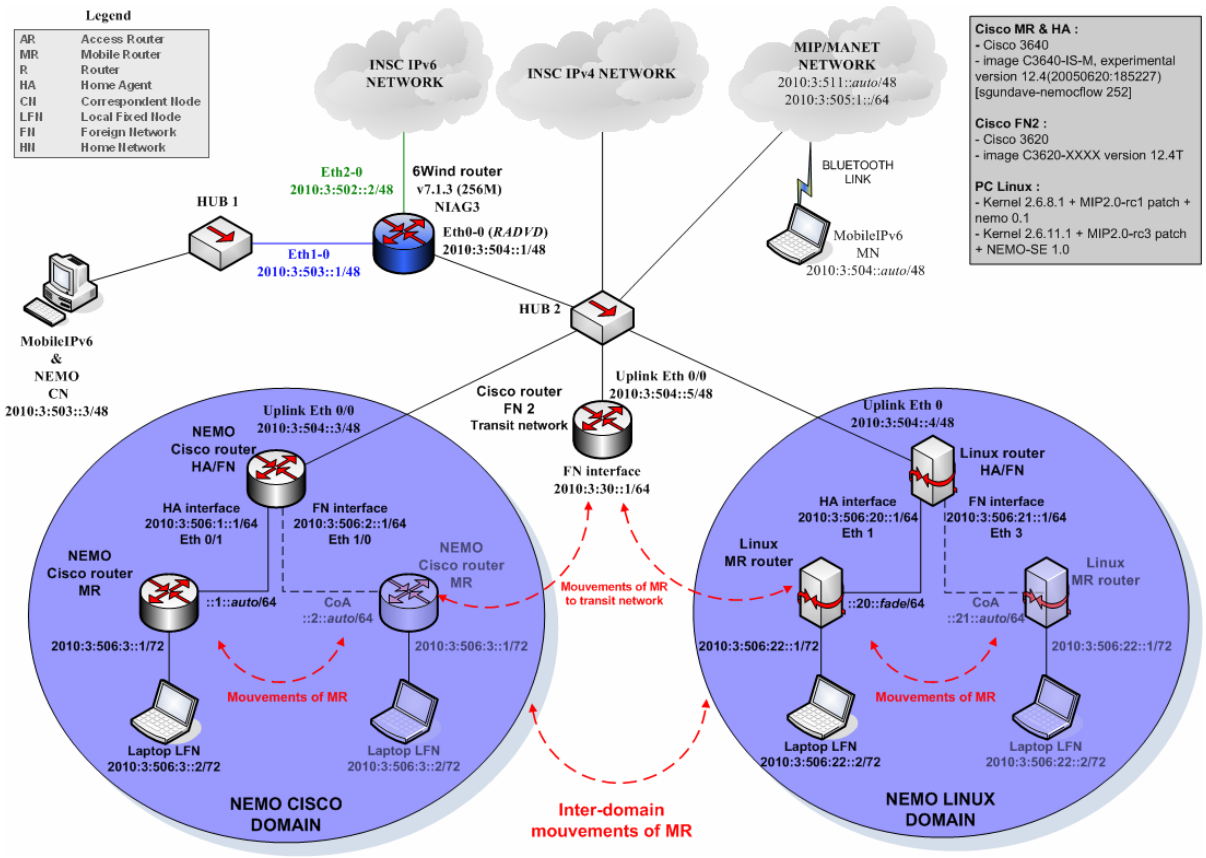

Figure 31: French platform for NEMO testbed

The Cisco platforms used for testing were 3640 routers using IOS C3640-IS-M experimental version 12.4 (20050620:185227). In the Linux environment, all machines were Linux PCs with kernel 2.6.11-1, MIPL 2.0-RC3 [58], NEPL-SE 1.0 [59] (based on NEMO daemon 0.1), and RADVD 0.9. These were the latest releases at the time, though newer versions of the software have been released based on newer kernels and NEMO daemons. The major difference between the FR testbed and those of the other POs resides primarily in the use of the Linux kernel 2.6.11-1 with MIPL2.0-RC3 patch, and NEPL-SE 1.0 instead of NEPL 0.1 and MIPL2.0-RC1 patch.

3.4 Linux NEMO Functionality Testing

The functional tests summarized in the following sections have been carried out in the GE testbed (see Figure 30, above), but the results obtained by GE have been confirmed by the experiments performed by IT and FR.

3.4.1 MR1 roaming between Home and Foreign Networks

The goal of this first functional test has been to analyze the correctness and stability of the NEMO protocol when a single mobile network dynamically changes its point of attachment to the WAN. For this test, the Mobile Router (MR1) continuously roamed among its home network and both foreign networks, while the CN continuously sent ICMPv6 echo request packets to the MR1's home address.

By monitoring of echo request and echo reply exchanges on the home network, it was verified that the NEPL NEMO implementation correctly provided the expected mobility support. Additionally, the sniffing station was able to display the respective NEMO control information, such as Binding Updates and Binding Acknowledgements exchanged between MR1 and HA. This information helped T3 members discover some issues with the current NEPL implementations, but these flaws will be discussed later.

3.4.2 Nested Mobility

The goal of this functional test was to analyze the correctness and stability of the nested NEMO functionality, that is, to show the proper protocol operation in the case where one MR is connected behind another. For this test, MR2 was connected to MR1's mobile network. MR1 continued to roam between the home and foreign networks, and thus the two mobile networks roamed together as a single, hierarchical mobility unit. During this test, the CN continuously sent ICMPv6 echo request packets to MR2's home address.

Monitoring the echo request/reply exchanges on the home network verified that the NEPL NEMO implementation correctly provided the expected nested mobility support up to a nesting level of 2. With some performance degradation due to additional levels of encapsulation, this nesting method should also work for higher levels of nesting.

3.4.3 Flaws Discovered in Linux Implementation

While the basic NEMO functionality did appear to work correctly as previously discussed, some flaws were discovered in the NEPL implementation.

3.4.3.1 Missing override flag in HA's proxy neighbor advertisement

When a MR leaves its home network and attaches to a visited network, it registers its new location with the HA. From this point on, the HA will act as a proxy for the MR, that is, it will intercept the packets destined for the MR and forward them to the registered CoA of the MR on the visited network.

In order to act as proxy, the HA is expected to send an ICMPv6 neighbor advertisement on the home network, with the target address set to the MR's home address, and the link layer address set to its own link layer address. Once all the systems on the home link update the entry for the MR in their neighbor cache, they will forward packets destined to the MR's home address directly to the HA. To force all systems to update their neighbor cache immediately, the HA should set the "override flag" in the respective ICMPv6 neighbor advertisement.

Using the NEPL NEMO implementation, the HA sends the appropriate neighbor advertisement, but does not set the override flag as shown in Figure 32. This results in the other systems on the home link not updating their neighbor caches immediately, and therefore continuing to send all packets addressed to the MR still to the MR's link layer address, until their respective neighbor caches entries expire. During this remaining expiration time, no packet destined to the MR will be sent to the HA, so the MR will lose packets because the HA is unable to forward them. In lab testing, the period of this packet loss varied between few seconds and about one minute, depending on the

remaining neighbor cache expiration time of the router of the home link at the time the MR leaves its home link.

```
Frame 103 (86 on wire, 86 captured)
    Arrival Time: Jan 18, 2006 17:45:46.995590000
    Time delta from previous packet: 0.322746000 seconds
    Time relative to first packet: 61.150029000 seconds
    Frame Number: 103
    Packet Length: 86 bytes
    Capture Length: 86 bytes
Ethernet II
    Destination: 33:33:00:00:00:01 (33:33:00:00:00:01)
    Source: 00:04:76:e8:bd:c7 (3_e8:bd:c7)
    Type: IPv6 (0x86dd)
Internet Protocol Version 6
    Version: 6
    Traffic class: 0x00
    Flowlabel: 0x00000
    Payload length: 32
    Next header: ICMPv6 (0x3a)
    Hop limit: 255
    Source address: 2010:2:102::131 (2010:2:102::131)
    Destination address: ff02::1 (ff02::1)
Internet Control Message Protocol v6
    Type: 136 (Neighbor advertisement)
    Code: 0
    Checksum: 0x6dbf (correct)
    Flags: 0x80000000
        1... .... .... .... .... .... .... .... = Router
        .0.. .... .... .... .... .... .... .... = Not adverted
        ..0. .... .... .... .... .... .... .... = Not override
    Target: 2010:2:102:0:202:2dff:fea9:e227 (2010:2:102:0:202:2dff:fea9:e227)
    ICMPv6 options
        Type: 2 (Target link-layer address)
        Length: 8 bytes (1)
        Link-layer address: 00:04:76:e8:bd:c7
```

HA is sender of Neighbor advertisement

Override flag is not set

Target address of Neigbor advertisement is home address of MR1

HA acts as proxy for MR1

Figure 32: Proxy neighbor advertisement sent from HA on behalf of MR1

3.4.3.2 Empty Home Agent List in DHAAD

To add more flexibility to the NEMO protocol, a HA does not have to be configured in a static way, but can also be detected dynamically, through a process called Dynamic Home Agent Address Discovery (DHAAD). Using DHAAD, the MR will not immediately register with a certain HA when connected to a visited network, but will first detect the appropriate HA to register with. To do this, it sends a DHAAD Request message to the HA's anycast address. The first HA receiving this DHAAD Request will answer with a DHAAD Reply to the requesting MR, and include in this reply a list of available HAs on the home link sorted by their preference to act as a HA. This information is obtained by the HAs from the router advertisements each HA is sending on the home link. The MR receiving the DHAAD Reply will then use the most preferred HA in the Home Agent List for registering its current location.

Testing performed by T3 members showed that MR1, when on foreign network FN1 (see Figure 30), was sending a DHAAD Request message to the HA. The HA received this message and replied as expected, but the Home Agent List to be included at the end of the DHAAD Reply was empty. MR1 was unable to select a HA from the empty Home Agent List in the DHAAD Reply, and was consequently unable to register its new

location. Due to this flaw, the basic network mobility support is not working when DHAAD is used.

3.5 NEMO Performance Testing

3.5.1 Handoff Analysis

NEMO performance may be studied through analysis of the signaling traffic flowing through the MR egress interface, which is triggered by the movements of the MR among the visited subnets. These tests were executed in the IT testbed (Figure 29 above) with a Cisco HA and both Cisco and Linux Mobile Routers. An active ping (one echo request per second) was used to recognize when bidirectional communications was reestablished between the LFN and its CN. As previously discussed, in order to minimize the delay due to the movement detection, the mean RADV rate was lowered to 500ms on all the visited networks (newer IOS versions allow the use of sub-second RADV rates). While a rough estimate of the handoff latency is also reported, a more analytic approach for that can be found in the next section.

3.5.1.1 Home Network → Foreign Network Handoff

3.5.1.1.1 Cisco Mobile Router

It was not possible to statically configure the Home Agent address in the Cisco implementation, so these tests had to be run using DHAAD on the Cisco platform. In this scenario, the MR is able to leave the home network correctly, but the DHAAD Request is sent with a very high delay (>35s in Figure 33), which markedly impairs the overall handoff latency. Other components of the latency are due to Duplicate Address Detection (DAD). There is a ~1s delay for DAD from the MR at its CoA, calculated from the time between the neighbor solicitation and the unsolicited neighbor advertisement. A second ~1s delay is due to DAD performed by the HA for the home address, which is approximated by the delay between the Binding Update (BU) and the Binding Acknowledgement (BA).

It is worth noting the anomalous delivery by the MR of Neighbor Solicitations to the address ff02::1:ffff:fffe; this behavior is not proper for MIPv6 or for the Neighbor Discovery protocol.

```
1.815787 2001:6b8:20:185:2d0:59ff:fe4b:7f6e -> 2001:6b8:20:1846:204:75ff:fee4:fc37  ICMPv6 Echo request
1.818302 2001:6b8:20:1846:204:75ff:fee4:fc37 -> 2001:6b8:20:185:2d0:59ff:fe4b:7f6e  ICMPv6 Echo reply
2.083852 fe80::2e0:1eff:fe7e:65e2 -> ff02::1                                        ICMPv6 Router advertisement
2.543834 fe80::2e0:1eff:fe7e:65e2 -> ff02::1                                        ICMPv6 Router advertisement
                                                  Handoff
3.025608 fe80::20c:31ff:feea:4b81 -> ff02::1                                        ICMPv6 Router advertisement
3.025981          :: -> ff02::1:ffb2:9d00                                           ICMPv6 Neighbor solicitation
3.486280 fe80::20c:31ff:feea:4b81 -> ff02::1                                        ICMPv6 Router advertisement
3.816306 2001:6b8:20:185:2d0:59ff:fe4b:7f6e -> 2001:6b8:20:1846:204:75ff:fee4:fc37  ICMPv6 Echo request
3.816312 2001:6b8:20:185:2d0:59ff:fe4b:7f6e -> 2001:6b8:20:1846:204:75ff:fee4:fc37  ICMPv6 Echo request
3.890960 fe80::20c:31ff:feea:4b81 -> ff02::1                                        ICMPv6 Router advertisement
4.023702 2001:6b8:20:1841:260:2fff:feb2:9d00 -> ff02::1                             ICMPv6 Neighbor advertisement
4.027960 2001:6b8:20:1841:260:2fff:feb2:9d00 -> ff02::1:ffff:fffe                   ICMPv6 Neighbor solicitation
4.351634 fe80::20c:31ff:feea:4b81 -> ff02::1                                        ICMPv6 Router advertisement
  ...
  ...
38.669645 fe80::20c:31ff:feea:4b81 -> ff02::1                                        ICMPv6 Router advertisement
38.809073 2001:6b8:20:185:2d0:59ff:fe4b:7f6e -> 2001:6b8:20:1846:204:75ff:fee4:fc37  ICMPv6 Echo request
39.026255 2001:6b8:20:1841:260:2fff:feb2:9d00 -> 2001:6b8:20:187:fdff:ffff:ffff:fffe ICMPv6 Dynamic Home Agent Address Discovery Request
39.029256 fe80::20c:31ff:feea:4b81 -> ff02::1:ffb2:9d00                              ICMPv6 Neighbor solicitation
39.029536 2001:6b8:20:1841:260:2fff:feb2:9d00 -> fe80::20c:31ff:feea:4b81            ICMPv6 Neighbor advertisement
39.030409 2001:6b8:20:187::1 -> 2001:6b8:20:1841:260:2fff:feb2:9d00                  ICMPv6 Dynamic Home Agent Address Discovery Reply
39.034174 2001:6b8:20:1841:260:2fff:feb2:9d00 -> 2001:6b8:20:187::1                  MIPv6 Binding Update
39.082317 fe80::20c:31ff:feea:4b81 -> ff02::1                                        ICMPv6 Router advertisement
39.514986 fe80::20c:31ff:feea:4b81 -> ff02::1                                        ICMPv6 Router advertisement
39.808877 2001:6b8:20:185:2d0:59ff:fe4b:7f6e -> 2001:6b8:20:1846:204:75ff:fee4:fc37  ICMPv6 Echo request
39.935646 fe80::20c:31ff:feea:4b81 -> ff02::1                                        ICMPv6 Router advertisement
40.046624 2001:6b8:20:187::1 -> 2001:6b8:20:1841:260:2fff:feb2:9d00                  MIPv6 Binding Acknowledgement
40.368325 fe80::20c:31ff:feea:4b81 -> ff02::1                                        ICMPv6 Router advertisement
40.788980 fe80::20c:31ff:feea:4b81 -> ff02::1                                        ICMPv6 Router advertisement
40.806098 fe80::260:2fff:feb2:9d00 -> fe80::20c:31ff:feea:4b81                       ICMPv6 Neighbor solicitation
40.806891 fe80::20c:31ff:feea:4b81 -> fe80::260:2fff:feb2:9d00                       ICMPv6 Neighbor advertisement
40.808732 2001:6b8:20:185:2d0:59ff:fe4b:7f6e -> 2001:6b8:20:1846:204:75ff:fee4:fc37  ICMPv6 Echo request
40.813690 2001:6b8:20:1846:204:75ff:fee4:fc37 -> 2001:6b8:20:185:2d0:59ff:fe4b:7f6e  ICMPv6 Echo reply
```

~38s

DAD

DHAAD

Registration

Figure 33: Home → Foreign handoff with Cisco MR

3.5.1.1.2 Linux Mobile Router

The handoff appears to be correct on the Linux implementation. As shown in Figure 34, the total handoff latency is approximately 5 seconds, as there is no delay for the DHAAD process. Unlike the Cisco test, DAD for the CoA is executed a second time, unnecessarily, due to the CoA being assigned to the tunnel interface. Another difference is the absence of unsolicited neighbor advertisements at end of the DAD, which are optional. Again, the delay from the delivery of the BU and the reception of the BA is ~1s due to the DAD executed by the HA for the home address.

```
0.999810 2001:6b8:20:185:2d0:59ff:fe4b:7f6e -> 2001:6b8:20:1846:204:75ff:fee4:fc37 ICMPv6 Echo request
1.002683 2001:6b8:20:1846:204:75ff:fee4:fc37 -> 2001:6b8:20:185:2d0:59ff:fe4b:7f6e ICMPv6 Echo reply
1.109168 fe80::2e0:1eff:fe7e:65e2 -> ff02::1                                       ICMPv6 Router advertisement
1.493277 fe80::2e0:1eff:fe7e:65e2 -> ff02::1                                       ICMPv6 Router advertisement
1.969076 fe80::2e0:1eff:fe7e:65e2 -> ff02::1                                       ICMPv6 Router advertisement
                                                  Handoff
2.464459 fe80::20c:31ff:feea:4b81 -> ff02::1                                       ICMPv6 Router advertisement
2.466896          :: -> ff02::16                                                   ICMPv6 Multicast Listener Report Message v2
2.689868          :: -> ff02::1:ff65:1578                                          ICMPv6 Neighbor solicitation
2.849011 fe80::20c:31ff:feea:4b81 -> ff02::1                                       ICMPv6 Router advertisement
3.237603 fe80::20c:31ff:feea:4b81 -> ff02::1                                       ICMPv6 Router advertisement
3.391739          :: -> ff02::1:ff65:1578                                          ICMPv6 Neighbor solicitation
3.706356 fe80::20c:31ff:feea:4b81 -> ff02::1                                       ICMPv6 Router advertisement
4.175108 fe80::20c:31ff:feea:4b81 -> ff02::1                                       ICMPv6 Router advertisement
4.552554 2001:6b8:20:1841:2d0:59ff:fe65:1578 -> 2001:6b8:20:187::1                 MIPv6 Binding Update
4.667849 fe80::20c:31ff:feea:4b81 -> ff02::1                                       ICMPv6 Router advertisement
5.000013 2001:6b8:20:185:2d0:59ff:fe4b:7f6e -> 2001:6b8:20:1846:204:75ff:fee4:fc37 ICMPv6 Echo request
5.084539 fe80::20c:31ff:feea:4b81 -> ff02::1                                       ICMPv6 Router advertisement
5.537226 fe80::20c:31ff:feea:4b81 -> ff02::1                                       ICMPv6 Router advertisement
5.566199 fe80::20c:31ff:feea:4b81 -> ff02::1:ff65:1578                             ICMPv6 Neighbor solicitation
5.566372 2001:6b8:20:1841:2d0:59ff:fe65:1578 -> fe80::20c:31ff:feea:4b81           ICMPv6 Neighbor advertisement
5.567268 2001:6b8:20:187::1 -> 2001:6b8:20:1841:2d0:59ff:fe65:1578                 MIPv6 Binding Acknowledgement
5.949899 fe80::20c:31ff:feea:4b81 -> ff02::1                                       ICMPv6 Router advertisement
6.000990 2001:6b8:20:185:2d0:59ff:fe4b:7f6e -> 2001:6b8:20:1846:204:75ff:fee4:fc37 ICMPv6 Echo request
6.005937 2001:6b8:20:1846:204:75ff:fee4:fc37 -> 2001:6b8:20:185:2d0:59ff:fe4b:7f6e ICMPv6 Echo reply
```

~5s

DAD

Registration

Figure 34: Home → Foreign handoff with Linux MR (no DHAAD)

When the Linux implementation is run with DHAAD rather than static HA configuration, the results are the same. Unlike the Cisco test, there is no delay in the DHAAD Request, and DHAAD does not add an appreciable delay because the Round Trip Times (RTTs) in the testbed were not significant. However, one malfunction was

frequently encountered: the MR fails to send the DHAAD Request, and thus the LFN loses connectivity permanently.

3.5.1.2 Foreign Network → Foreign Network

3.5.1.2.1 Cisco Mobile Router

This handoff appears to be correct. No significant delay is present between the delivery of the BU and the reception of the BA. The Home Agent does not have to execute DAD for the home address.

3.5.1.2.2 Linux Mobile Router

The handoff appears to be correct and, like the previous case, the interval between BA and BU is not significant. Inspecting the packets showed that in both implementations, the movement detection algorithm is of *eager-cell* type, i.e. the reception of a new RA preemptively triggers the handoff without verifying the validity of old routers through Neighbor Unreachability Detection (NUD).

The BU is sent with a 2s delay from the delivery of the Neighbor Solicitation relating to the second DAD. As DAD duration in Linux is 1s, it may be concluded that the implementation introduces an unjustified and significant delay.

3.5.1.3 Foreign Network → Home Network

3.5.1.3.1 Cisco Mobile Router

As shown in Figure 35, returning home is problematic with the Cisco NEMO implementation. The MR does not send the deregistration BU, and thus the connectivity can be reestablished only when the home registration binding on the HA (lifetime 28s) expires.

```
 2.422457 2001:6b8:20:185:2d0:59ff:fe4b:7f6e -> 2001:6b8:20:1846:204:75ff:fee4:fc37 ICMPv6 Echo request
 2.427546 2001:6b8:20:1846:204:75ff:fee4:fc37 -> 2001:6b8:20:185:2d0:59ff:fe4b:7f6e ICMPv6 Echo reply
 2.551838 fe80::204:9aff:fe1d:a881 -> ff02::1                                       ICMPv6 Router advertisement
                                          Handoff
 3.134980 fe80::2e0:1eff:fe7e:65e2 -> ff02::1                                       ICMPv6 Router advertisement
 ...
 ...
 9.274533 fe80::2e0:1eff:fe7e:65e2 -> ff02::1                                       ICMPv6 Router advertisement
 9.420727 fe80::260:2fff:feb2:9d00 -> fe80::2e0:1eff:fe7e:65e2 ICMPv6               Neighbor solicitation
 9.421060 2001:6b8:20:185:2d0:59ff:fe4b:7f6e -> 2001:6b8:20:1846:204:75ff:fee4:fc37 ICMPv6 Echo request
 9.670645 fe80::2e0:1eff:fe7e:65e2 -> ff02::1                                       ICMPv6 Router advertisement
10.074451 fe80::2e0:1eff:fe7e:65e2 -> ff02::1                                       ICMPv6 Router advertisement
10.420616 fe80::260:2fff:feb2:9d00 -> fe80::2e0:1eff:fe7e:65e2                      ICMPv6 Neighbor solicitation
10.420746 2001:6b8:20:185:2d0:59ff:fe4b:7f6e -> 2001:6b8:20:1846:204:75ff:fee4:fc37 ICMPv6 Echo request
10.538423 fe80::2e0:1eff:fe7e:65e2 -> ff02::1                                       ICMPv6 Router advertisement
 ...
 ...
13.182205 fe80::2e0:1eff:fe7e:65e2 -> ff02::1                                       ICMPv6 Router advertisement
13.420159 fe80::260:2fff:feb2:9d00 -> ff02::1:ff7e:65e2                             ICMPv6 Neighbor solicitation
13.650211 fe80::2e0:1eff:fe7e:65e2 -> ff02::1                                       ICMPv6 Router advertisement
14.098128 fe80::2e0:1eff:fe7e:65e2 -> ff02::1                                       ICMPv6 Router advertisement
14.416855 fe80::260:2fff:feb2:9d00 -> ff02::1:ff7e:65e2                             ICMPv6 Neighbor solicitation
14.598157 fe80::2e0:1eff:fe7e:65e2 -> ff02::1                                       ICMPv6 Router advertisement
 ...
30.447736 fe80::260:2fff:feb2:9d00 -> ff02::1:ff7e:65e2                             ICMPv6 Neighbor solicitation
30.449002 fe80::2e0:1eff:fe7e:65e2 -> fe80::260:2fff:feb2:9d00                      ICMPv6 Neighbor advertisement
30.449335 2001:6b8:20:185:2d0:59ff:fe4b:7f6e -> 2001:6b8:20:1846:204:75ff:fee4:fc37 ICMPv6 Echo request
30.450647 2001:6b8:20:185:2d0:59ff:fe4b:7f6e -> 2001:6b8:20:1846:204:75ff:fee4:fc37 ICMPv6 Echo request
30.451797 2001:6b8:20:1846:204:75ff:fee4:fc37 -> 2001:6b8:20:185:2d0:59ff:fe4b:7f6e ICMPv6 Echo reply
```

~28s

Figure 35: Foreign → Home handoff with Cisco MR

3.5.1.3.2 Linux Mobile Router

In the Linux implementation, the MR erroneously executes DAD for the home address when returning home. Additionally, the BA sent by the (Cisco) HA is malformed, as it lacks the Mobility Header. The packet interpreted as “IPv6 IPv6 routing” as shown in Figure 36. However, the entry in the Binding Cache is deleted and thus the connectivity can be reestablished.

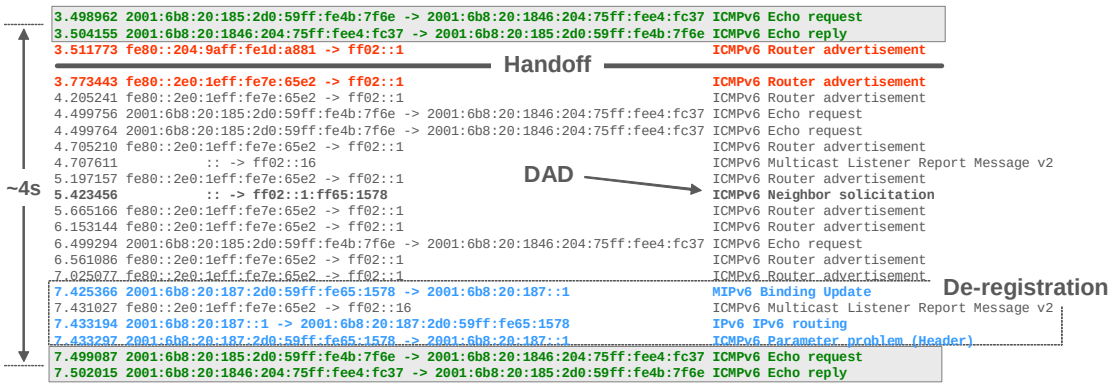

Figure 36: Foreign → Home handoff with Linux MR

3.5.2 Handoff Latency

This section summarizes the results of a simple measurement study directed at obtaining an estimate of the handoff latency. Again, these measurements were carried out in the IT testbed (Figure 29 above).

The handoff latency is defined in this context as the interval between the last echo reply received on the old link and the first one received on the new link. The estimate is calculated as the average of this interval over a series of ten handoffs (for each typology). The echo replies refer to an active ping between the LFN and the CN with a rate of ten echo requests per second, resulting in an accuracy of 200ms in the estimate.

The trials were parameterized by the RADV rate in order to highlight the movement detection contribution to the overall latency. Another contribution to the latency is the layer 1/layer 2 delay necessary for the switch to change the VLAN associated with the MR’s port; a good estimate of it may be considered 500ms.

The cases where an implementation did not operate correctly in the previous section (i.e., Cisco MR leaving/returning home) were excluded from this analysis, while for the cases with semi-correct behavior (i.e., Linux MR leaving/returning home), a single value was chosen for the RADV rate. The resulting handoff delays are shown in Table 1.

	Cisco MR		Linux MR					
	FN → FN		FN → FN		HN → FN		FN → HN	
RA rate	Avg	Std. Dev.	Avg	Std. Dev.	Avg	Std. Dev.	Avg	Std. Dev.
0.5s	**1.91**	0.17	**3.29**	0.55	**4,60**	0,67	**3,26**	0,41
1.5s	**2.38**	0.51	**3.99**	0.72	x	x	x	x
4.5s	**3.47**	0.99	**4.46**	1.08	x	x	x	x

Table 1: Handoff latency measurements

In the FN → FN scenario, the 1-1.5s difference between the Cisco and Linux MR can be attributed, as previously discussed, to the delay with which the Linux implementation sends a BU after DAD ends. For the Linux MR, the HN → FN scenario shows an additional ~1s delay, compared to the FN → FN case, due to DAD for the home address being executed by the HA before sending the BA. As the Linux MR erroneously executes the DAD for the home address, the FN → HN scenario is not actually different from the FN → FN case, as confirmed by the obtained measurement. Figure 37 shows a graph of the parameterized values for the FN → FN scenario for easier comparison of the performance of the Cisco and Linux NEMO implementations.

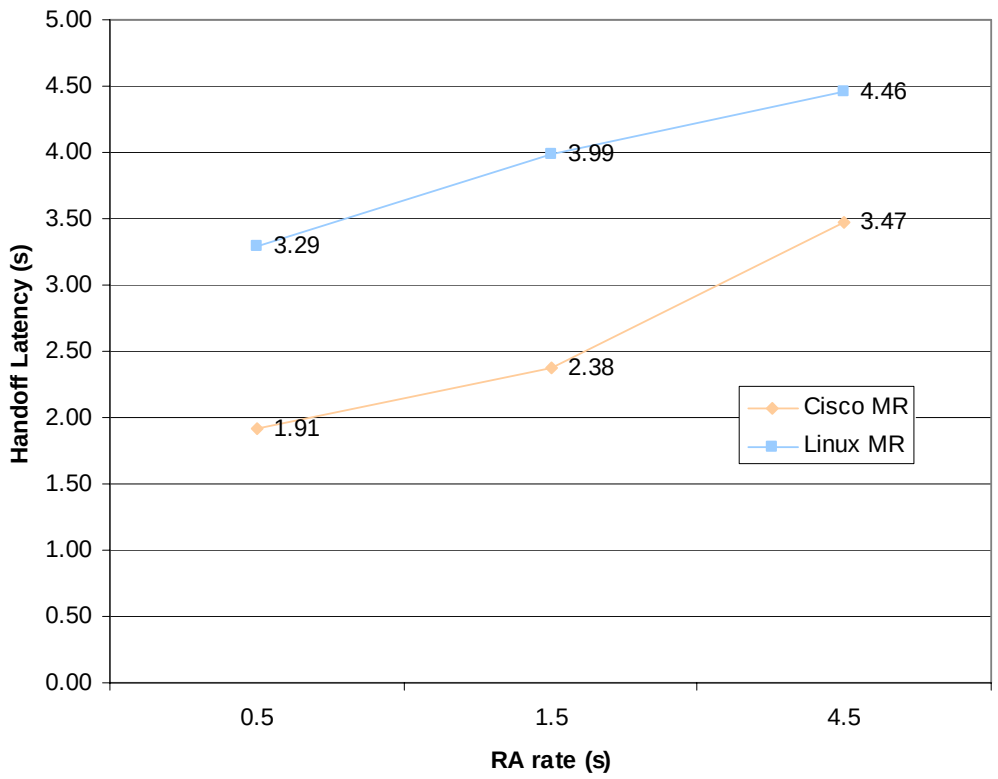

Figure 37: Handoff latency (FN → FN scenario)

3.5.3 Nested NEMO Performance

FR carried out a series of tests to measure the impact of nested NEMO tunnels on handover latency. The main purpose of the testing was to verify that double encapsulation had measurable effects on the handoff performance of network mobility. These tests were done with the Cisco and Linux NEMO implementations, used both separately and in an interoperable manner. The results are presented in the table and figure below.

	Average Handoff Latency (sec)	Standard Deviation (sec)	Median Handoff Latency (sec)
Cisco-Cisco	8.543	0.005	8.542
Nested Cisco-Cisco	10.544	0.005	10.545
Linux-Linux	2.392	0.166	2.380
Nested Linux-Linux	2.606	0.292	2.584
Linux MR - Cisco HA with DHAAD	4.261	0.183	4.272
Nested Linux MR - Cisco HA with DHAAD	4.524	0.355	4.413
Linux MR – Cisco HA without DHAAD	4.218	0.204	4.142
Nested Linux MR - Cisco HA without DHAAD	4.353	0.335	4.270

Table 2: Nested NEMO Handoff Analysis

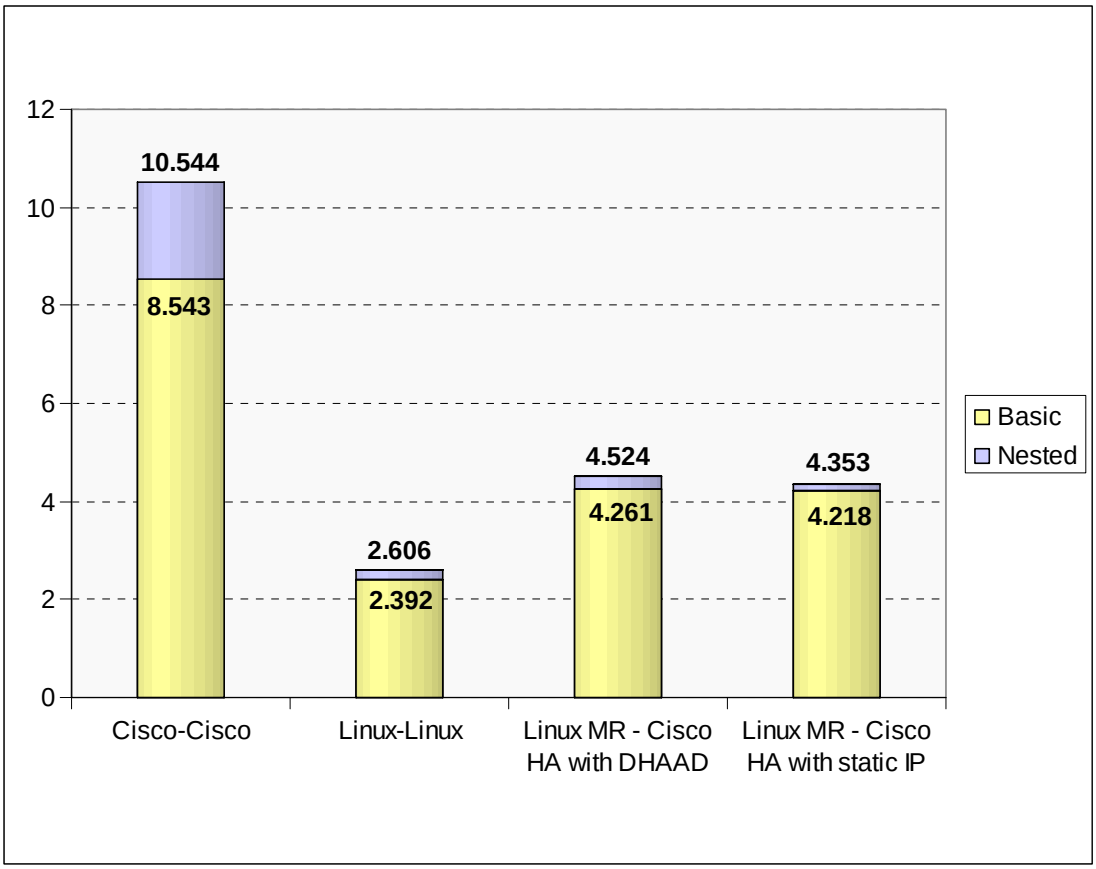

Figure 38: Nested NEMO Handoff Latency

For these tests, the mobile networks were simultaneously moved. The results show that the impact of the double encapsulation is minimal. The increased handoff latency is only due to the fact that both routers must send BUs and wait for BAs. In the case of the Cisco MR, it seems that the substantial handoff latency increase is due to the disconnection of the interface, which in turn increases the time necessary for the transmission of NEMO messages.

These tests constitute only a first stage of investigation, and more testing should be done with more advanced scenarios, such as higher levels of nesting and handoffs between points of attachment with different levels of nesting. It is also necessary to estimate the impact of the additional tunnels on the bandwidth and thus on the effective Maximum Transmission Unit (MTU) in such configurations, in order to be able to make useful recommendations for network architects.

3.5.4 Application Performance

To estimate the impact of the handoff on the functioning of various applications, several tests were carried on the FR testbed. The main goal of these tests was to analyze the effects of networks movements with different handoff delays on connection-oriented protocols such as Secure Shell (SSH) and File Transfer Protocol (FTP). To carry out these tests, a CN was placed in the fixed network. A connection was then established

between the CN and a Local Fixed Node (LFN) behind the MR. Figure 39 shows the results for short handoff latencies.

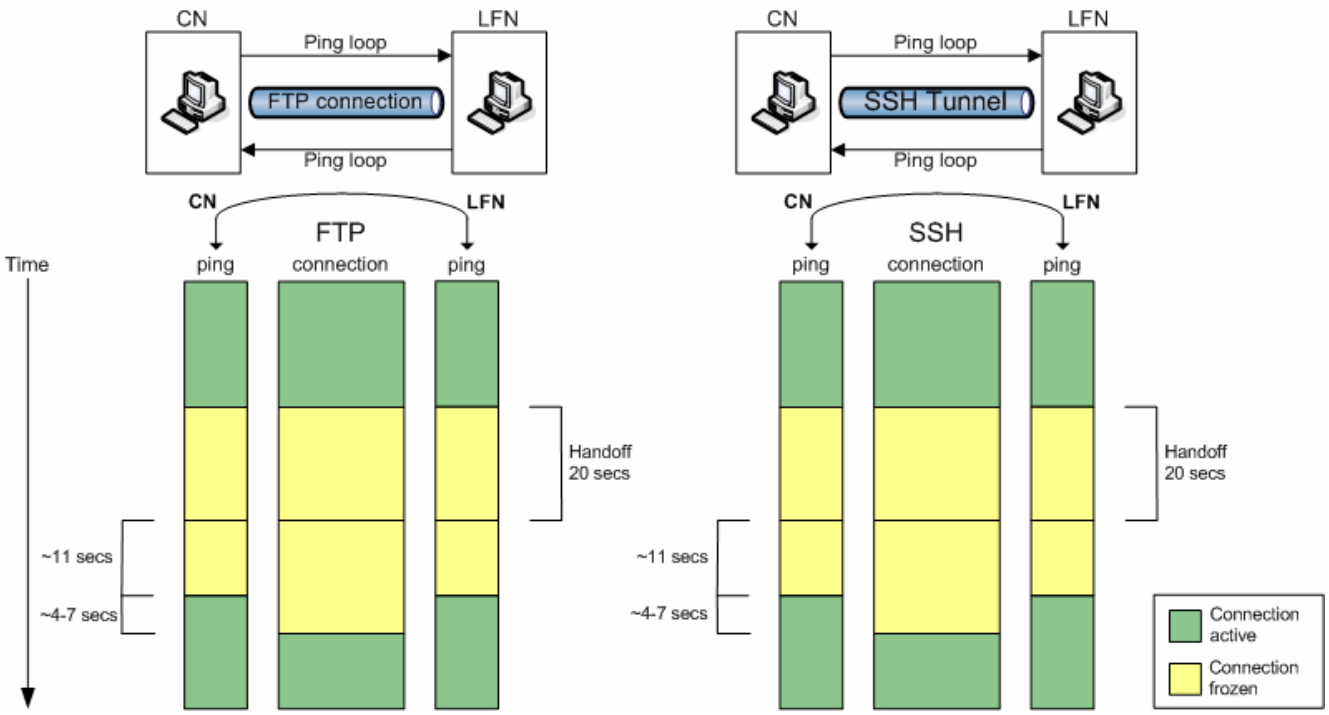

Figure 39: NEMO Impact on Applications (short handoff)

This test was carried out with various handoff delays (2-20 seconds) in basic and nested mode, and the same results were obtained with only small variations (1-2 sec). No unexpected effects were noticed during these tests: connections were not broken and the data transfers resumed correctly after 15-20 seconds.

However, when handoff delays grow larger, some broken connections were experienced with FTP, as shown in Figure 40.

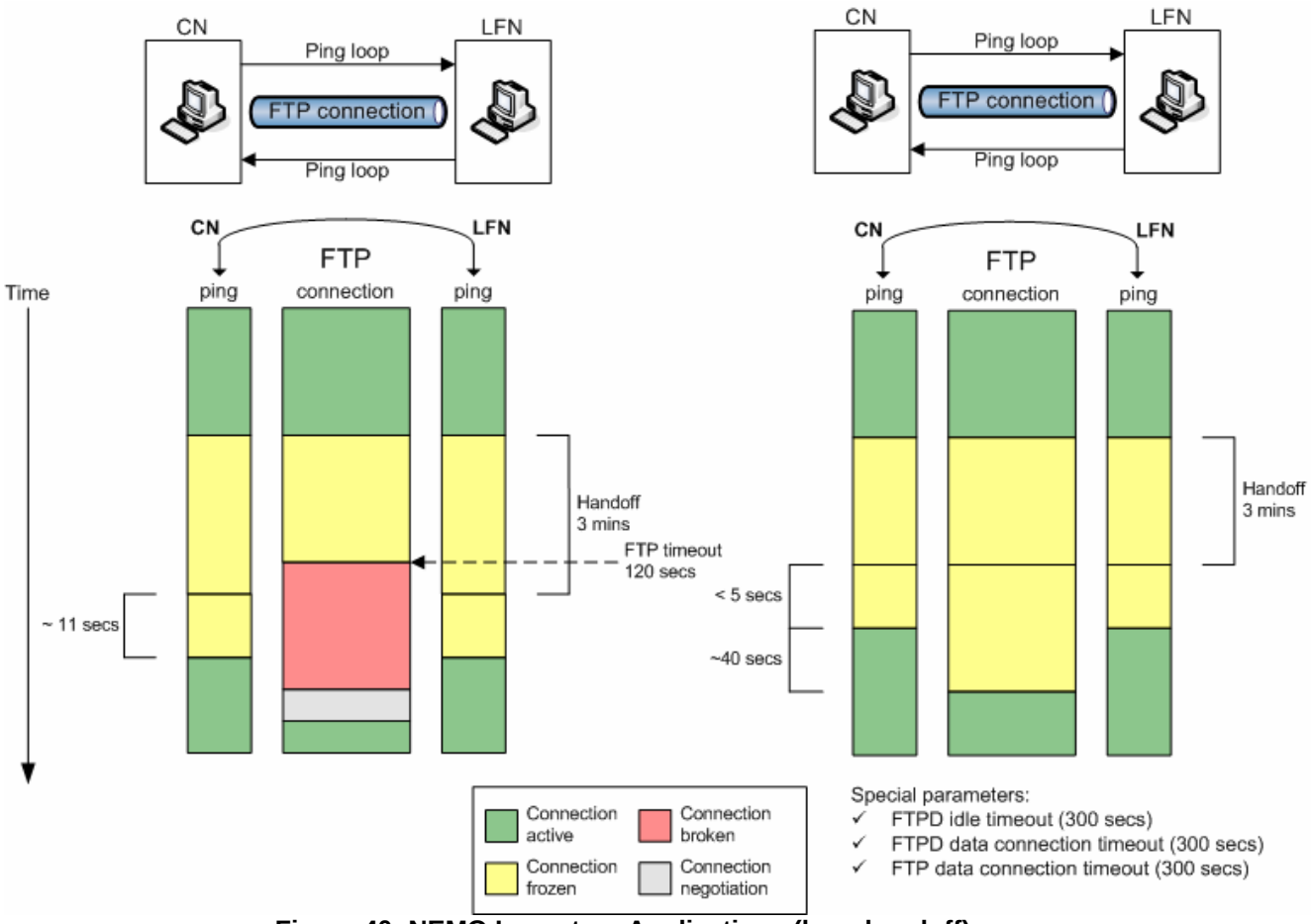

Figure 40: NEMO Impact on Applications (long handoff)

When the handoff latency exceeds the FTP server idle timeout, the connection is broken and must be renegotiated, which results in a larger delay to retrieve data. Once the FTP server parameters were increased to cover this extra delay, a second trial run showed that the connection remained unbroken and resumed correctly as before.

Network mobility does not have a significant impact on application protocols if they are configured to cope with an appropriate level of delay. However, there are significant potential impacts from NEMO on pseudo-real-time applications such as VoIP and video conferencing, where the delay or temporary interruption of service is not acceptable.

3.6 NEMO Conclusions

NEMO is a relatively new IETF proposed standard and, as such, suffers to some extent from lack of maturity. While the plain reuse of Mobile IPv6 accelerated the standardization process, perhaps it was not the optimal technical solution as MIPv6 was intended for hosts and not for routers. For example, there is only one tunneling option (IPv6-in-IPv6) between the MR and the HA. However, a good amount of work is underway in IETF to refine the protocol and to fill in the missing parts (e.g., multihoming, IPv4/NAT traversal, route optimization).

The current NEMO implementations are still in an experimental state, though as the German field trial demonstrated, they can actually be deployed in (selected) real scenarios, keeping in mind the issues summarized in the previous section. The NEMO level 2 nesting functionality works well, suggesting that further levels of nesting should work as well. It should to be noted, however, that each nesting level adds a non-negligible overhead to each data packet (40 bytes per level) for the additional encapsulating IPv6 header. The QoS seems to be slightly degraded for increased levels of nesting.

The obtained performance shows that the handoff latency may be too high for many real-time applications like VoIP and video conferencing. As demonstrated by the measurements, the MIPv6 protocol adds approximately 1.5s of latency in the best case, which may be too much to deliver an uninterrupted service for real-time communications. The main sources of delay are the latencies due to the DAD procedure and the naïve IP-based movement detection algorithm used in both implementations. Moreover, the high Router Advertisement rate required on the access network is not always desirable in lower bandwidth type radio links.

In future work, it would be interesting to investigate NEMO enhancements that are defined in the standard as extended features. Techniques such as route optimization could improve NEMO performance, and may eventually become part of the NEMO standard. Further information on Task3 NEMO testing and results may be found in [60].

4 Hybrid MANET-Edge System Mobility

4.1 MANET-MIPv6

IT studied and proposed a solution for integration of Mobile IPv6 within ad-hoc networks. The use of Mobile IPv6 within MANET is considered necessary to retain sessions in an environment where MANET nodes are endowed with several global addresses which can become unavailable after a significant topological event. Indeed, in such cases, a MANET node may change its configured global address and then experience an interruption of its active sessions. The proposed solution is based upon the OLSR routing protocol endowed with global address autoconfiguration extensions as described on page 29. It is assumed that the autoconfiguration protocol configures all available global addresses on the MANET interface.

The integration work cannot be a porting of MIPv6, since that protocol has been developed for use in LANs, where the devices (Access Routers) providing global connectivity information are on the same layer 3 (IP) link as the Mobile Node (MN). In MANETs, global connectivity information is provided by gateways, which can be separated from a generic MANET device by multiple wireless hops. Therefore, all link-local messages used by MIPv6 in a LAN environment to get connectivity information cannot be used within a MANET.

The relevant elements of MIPv6 that must be considered for the integration are the following:

- Home Network information set: each node must know its Home Address and its Home Agent (HA). The current solution uses a static method (from configuration file).
- Visited Network information set: each node must automatically configure at least one Care of Address (CoA). IT's global address auto-configuration solution described above accomplishes this task.
- Connectivity between HA and CoA must be guaranteed. Within the MANET, this is guaranteed by OLSR and MID messages generated by the autoconfiguration module; within the external network, data packet forwarding is enabled by the routing protocol of the infrastructure network (e.g. OSPF, RIP).
- There must be a movement detection procedure, which indicates MIPv6 handover execution and triggers registration of a new CoA with the HA.

The main issue of implementing MIPv6 inside a MANET is the movement detection procedure, which uses router advertisements (RADV) and Neighbor Unreachability Detection (NUD) for standard MIPv6 operation. Such procedures and messages are not available in ad-hoc networks, but their tasks and information can be obtained. Prefix discovery is provided using distributed RADV or by distributing prefix advertisements using OLSR or SMF, as described in the IT-proposed autoconfiguration solution, and gateway connectivity can be monitored by the OLSR routing protocol. Thus, we have everything necessary to detect motion and execute a handover.

Moreover, if several global addresses are available to a MANET device, the choice of the CoA that will be registered with the Home Agent affects the path followed within the MANET by the downlink traffic, and therefore impacts in the overall achievable performance. If the chosen path is the optimal one, MANET bandwidth resources are exploited in an efficient manner. In order to cope with this goal, the movement detection procedure of the IT MANET-MIPv6 solution takes performance metrics (i.e. routing metrics associated with available gateways) into account when making handover decisions, along with the connectivity status of the gateway associated to the registered CoA. As a consequence, downlink traffic path optimization fulfillment implies handover events even if the currently used gateway is still reachable. It is worth noting that in LAN/WLAN environments there is no downlink path problem; the MN can change its CoA only after losing connectivity with its default router (which is the device announcing the global prefix associated to the changed CoA).

Table 3 summarizes the main differences between standard MIPv6 and MANET-MIPv6 solution.

	LAN – MIPv6 standard	MANET – MIPv6 IT solution
Connectivity towards external network	Neighbor Unreachability Detection and Router Advertisements	OLSR HNA messages and prefix advertisements (distributed RADV, PA messages)
Prefix Discovery / CoA configuration	Router Advertisements	prefix advertisements (distributed RADV, PA messages) and Global address configuration solution
Downlink traffic path optimization	Not necessary within single hop environments	Considered in CoA selection

Table 3: Standard MIPv6 vs. MANET MIPv6 comparison

The set of the key operations and fundamental aspects considered by movement detection for the handover decision are the following:

- MANET node is aware of all prefixes and gateways addresses (Prefix Discovery) – all the correspondent global addresses are configured on its interface;
- MANET node interacts with routing protocol to obtain the metrics associated to the gateways, i.e. the number of hops;
- Metrics associated to those gateways are associated to the prefixes;
- MANET node chooses the best prefix among those available, registering to its HA the corresponding global address as Primary CoA (Best CoA Selection algorithm, BCS)
- Best prefix selection can be executed using the default gateway, but can also use hysteresis to prevent the node from re-registering often under mobility.

Mobile IPv6 executes the BCS algorithm and selects the (new) CoA to register with HA when there is a loss of connectivity towards the gateway associated to the registered CoA. This change of CoA is mandatory to maintain connectivity between MANET node and the external network. The loss of connectivity can be detected via a variety of methods, including HNA validity timers and routing table information. Additionally, a new CoA can be selected when there is a change to some metrics related to the gateways. In this situation, the change of CoA may optimize the downlink path, but it isn't mandatory since the gateway associated with the prefix currently in use is still reachable by the MANET node.

4.1.1 Examples

Some examples are provided in order to clarify the way MANET MIPv6 movement detection works. For each of the scenarios included, the list of operations made by the MANET node is given. The three significant scenarios included are:

- Bootstrapping
- Loss of connectivity toward the gateway associated to the registered CoA
- Downlink path optimization

At bootstrap time the MANET node does not have any information about the MANET and, in particular, about the gateways. So, it:

- Configures a MANET-local address on its interface and uses it as Originator Address for the routing protocol;
- Participates to OLSR and to the Prefix Discovery mechanism;
- When it receives the first PA, it builds a global address and registers it to the HA, because it is the only CoA and so the BCS returns it as the best one;
- This CoA is broadcasted in the MANET through the MID by OLSR
- Now the MANET node can communicate with any host using its Home Address

Obviously, there is no guarantee about the performance achievable using this CoA, so the MANET node may re-execute the BCS after receiving information (i.e. available prefixes) related to other gateways.

Several events may trigger the loss of connectivity towards the gateway associated with the prefix currently used by the MANET node to build the registered CoA. These events include MANET partitioning, a gateway failure (Figure 41), or a gateway turning into a node after having lost connectivity towards the external network. In each of these cases, the significant operations are the following:

- The registered CoA is considered invalid after the expiration of the validity timer of its correspondent prefix
- The MANET node re-executes the BCS algorithm among the valid prefixes and selects the best one
- The MANET node registers the CoA derived from the best prefix with its HA.

It is worth noting that when the timer expires, if the MANET node already knows all the information about the other gateways (if any), it can register another CoA immediately. On the other hand, if the loss of connectivity is due to a transition from one MANET to another, there is a transient period necessary for the node to receive the prefixes of the new MANET. In this case, the scenario is similar to the bootstrap one, but no site-local address configuration is required.

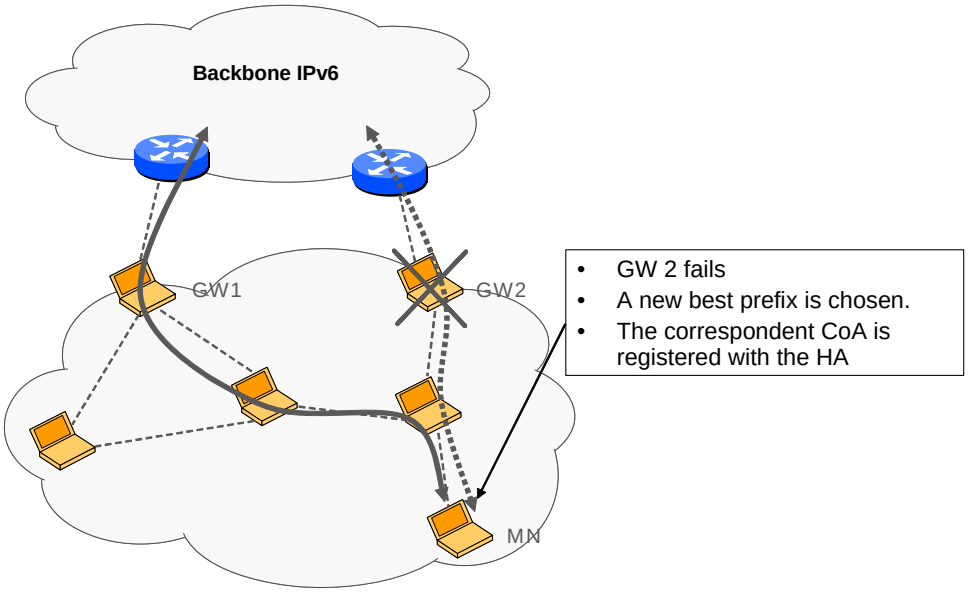

Figure 41: Execution of handover after a gateway failure

If the MANET node realizes that, after a topology variation, the currently-selected gateway is not the optimal one, it may decide to register another CoA to re-optimize the downlink path (Figure 42). In particular, the IT solution checks that the register CoA optimizes the downlink path each time some topological change involving one of the gateways is experienced. The set of the operations executed are the following:

- OLSR realizes that the metrics of some gateways have changed
- The MANET node re-executes the BCS algorithm and selects the best CoA
- If the best CoA isn't the registered one, the MANET node registers the new CoA to its HA.

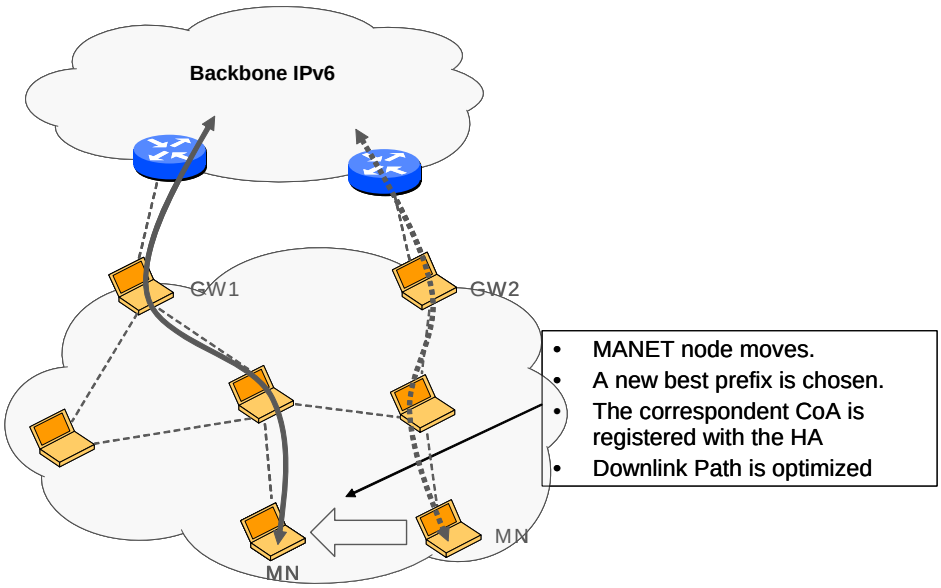

Figure 42: Execution of handover for downlink path optimization

With the exception of the bootstrap scenarios and the case in which the node changes MANETs, the latency introduced by a global address change is minimized (ideally it is reduced to zero), granting better performances with MIPv6 use. This is achieved by the global address configuration mechanism described earlier. In fact, if a node experiences a change from a first gateway to a second gateway, then it chooses a new global address associated with the second gateway, and it updates the CoA at its HA with a Binding Update (BU). The HA acknowledges to the MANET node the registration by sending back a message (named Binding Acknowledgment, BA) destined to the MANET node CoA. The BA message from the HA arrives to the gateway and is immediately routed to the node, since a proper route is already available. If the route towards the new CoA is not set up (such as in MANET change), the expected BA may not be received and the MANET node will have to retransmit the BU.

The proposed solution is therefore suitable for global connectivity provisioning and active session maintenance in scenarios where a MANET has several gateways and a high degree of mobility. In such scenarios, the use of a distributed routing solution announcing routes to MANET nodes within the Core Network might not be feasible due to scalability limits by which Mobile IPv6 is not affected. With the MANET MIPv6 solution, bandwidth resources are optimized both for uplink traffic (by OLSR HNA messages) and for downlink traffic (by the BCS algorithm) without introducing significant delay during handovers (IT global address Autoconfiguration solution). The main drawback is the Home Agent role, which is a centralized point of failure of the network.

4.1.2 Testing Results

The proposed solution has been implemented using the MIPL implementation of MIPv6 and tested for functionality and performance measurements. The main objectives of the experimental activity were validation of the benefits introduced by downlink path optimization and evaluation of the level of responsiveness to topology changes involving gateways.

Two main scenario types have been emulated in order to induce significant events triggering the Movement Detection. The scenarios are:

- topology variation inducing a change of downlink traffic path
- the failure of the gateway used to receive downlink traffic

In each test, MIPv6 was installed on only one MANET terminal (the Mobile Node) and a fixed MGEN UDP stream was transmitted by the CN, a terminal located outside the MANET, towards the MANET node Home Address. The flow towards the MN was in Bidirectional Tunneling and the IPSec was disabled. The main OLSR simulation parameters were the messages generation intervals, described in Table 4.

Hello messages emission interval	1 second
TC messages emission interval	2 seconds
HNA messages emission interval	2 seconds
PA messages emission interval	2 seconds
MID messages emission interval	5 seconds
Hysteresis mechanism	Enabled with default values

Table 4 Main OLSR parameters

The first scenario is a change in the downlink traffic path caused by topology variation. As shown in Figure 43, the MIPv6 MANET node moves through the MANET and optimizes its downlink path by selecting the CoA corresponding to the closest default gateway. In this scenario, measurements of throughput and handover latency have been taken; the rate of the MGEN flow was slightly lower than the estimated saturation value.

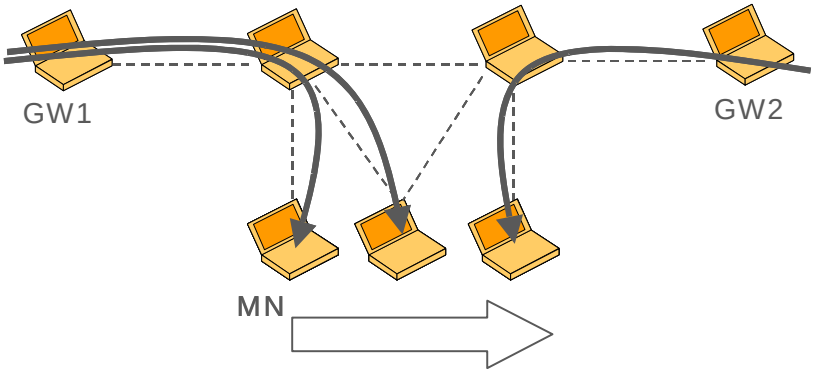

Figure 43: topology with downlink path optimization

The measured throughput is reported in Figure 44. Four topology events triggering handovers (caused by four changes of default gateway and registered CoA) can be noticed. In these intervals, the MIPv6 MANET node cannot receive any data, and the measured throughput is zero as expected. When the MIPv6 MANET node is reconnected to its HA, it receives, on average, all the packets sent by the CN (the dot line represents the data rate), independently from the registered CoA.

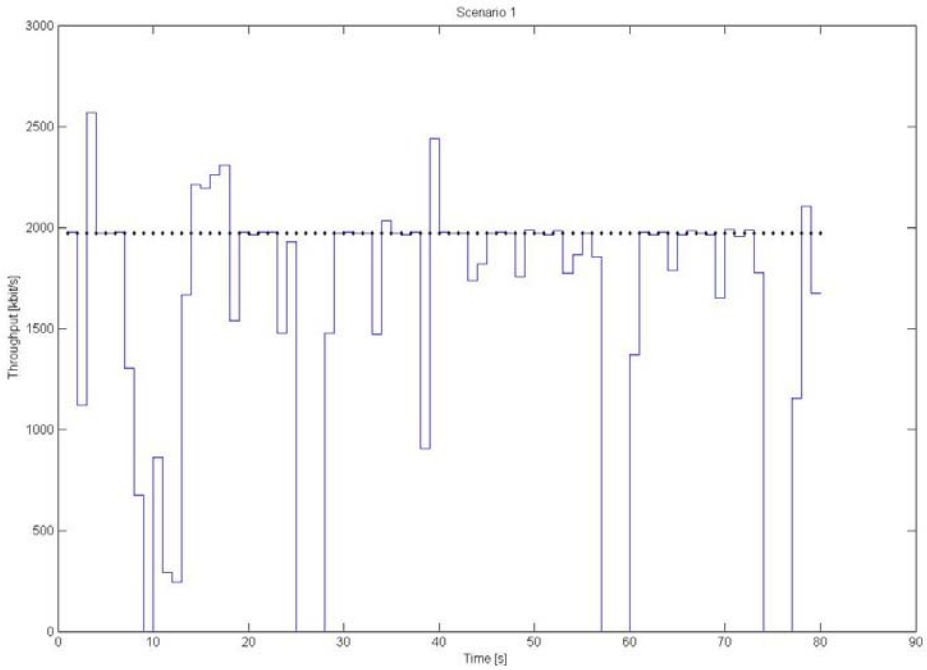

Figure 44: Throughput with downlink path optimization

Figure 45 reports the relation between the handover latency and the number of BUs sent by the MIPv6 MANET node to register the new CoA in each handover so that the handovers characterized by the use of back-off exponential algorithm can be identified. About fifty handovers have been emulated during measurements sessions. The solid line is the average value of the handover latency and the dotted lines are the average handover value plus/minus its standard deviation.

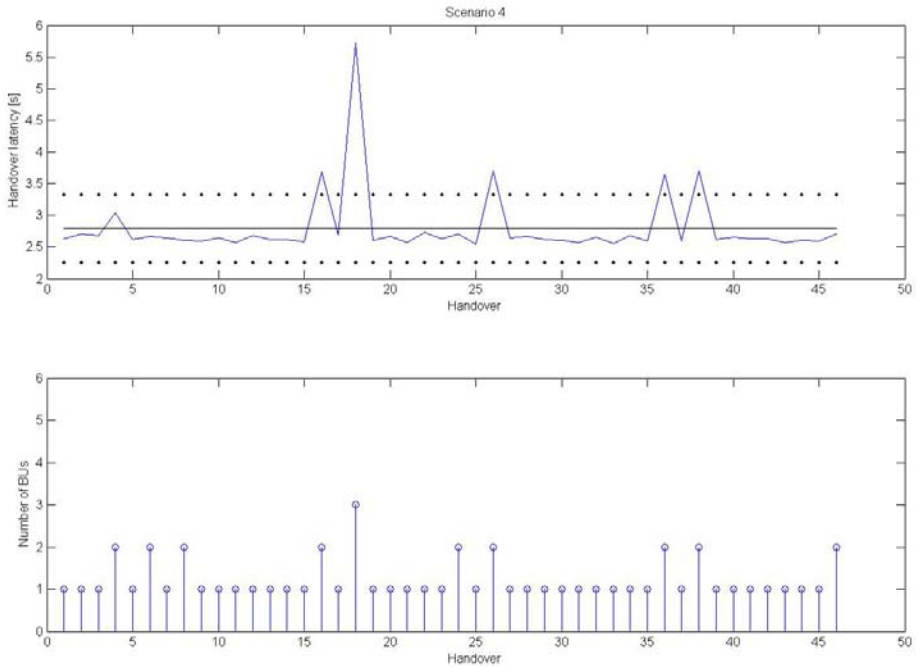

Figure 45: Handover latency with downlink path optimization

It can be noticed that the handover latency increases significantly when MIPv6 hast to retransmit the BU because the first one was not delivered to the Home Agent due to interference, routing problems, etc. If the registration succeeds at the transmission of the first BU, the handover interval depends only on the routing protocol timing and is not affected by MIPv6.

The second scenario, the same as the first, but with no downlink path optimization, is illustrated in Figure 46. The MIPv6 MANET node moves within the MANET (as in the first one), but it always uses the same CoA. Therefore, the downlink traffic always flows always the same gateway, and the downlink path is not always optimized. The rate of the data traffic is the same as the first scenario.

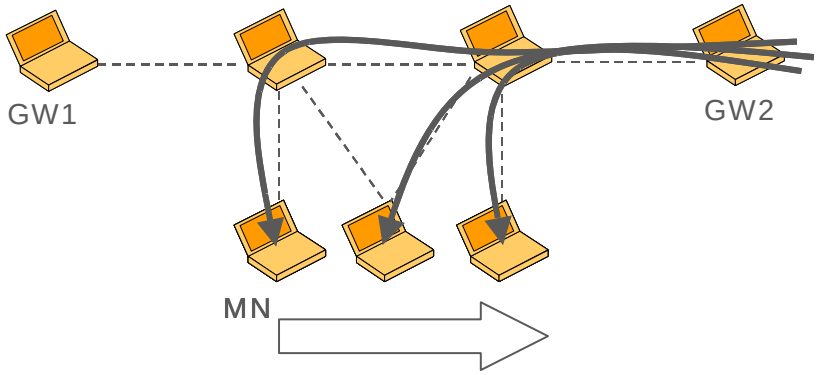

Figure 46: topology without downlink path optimization

Measured throughput is reported in Figure 47. The impact of a non-optimized downlink path can be easily noticed. When the MIPv6 MANET node uses a gateway that isn't the closest one, about 20% of packets are lost (this can be noticed by comparing Figure 47 with Figure 44).

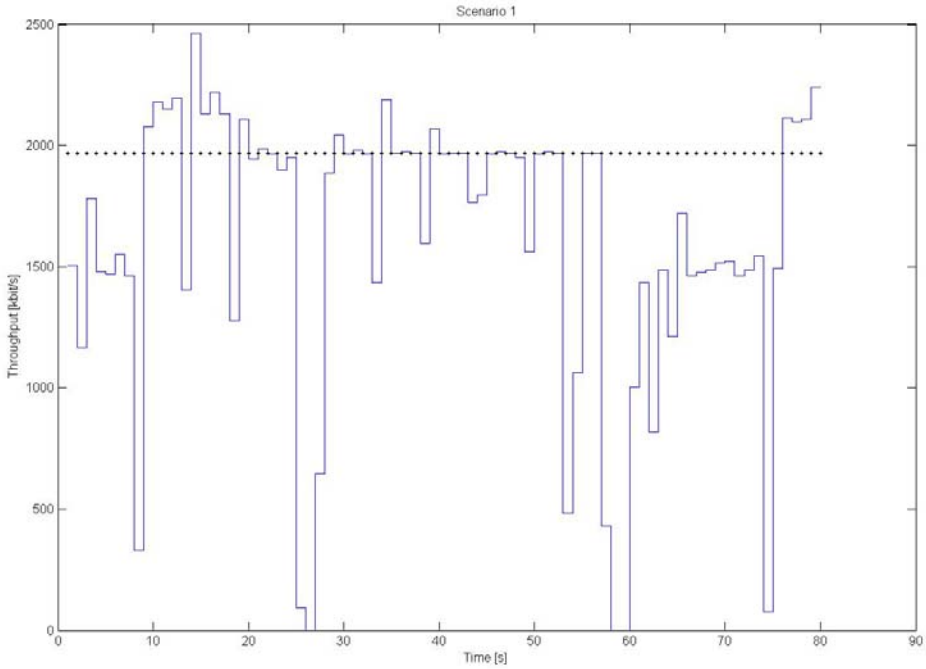

Figure 47: Throughput without downlink path optimization

Figure 48 illustrates the third scenario, in which the gateway associated to the prefix of the CoA registered by MIPv6 MANET node fails, and a new CoA already owned has to be registered.

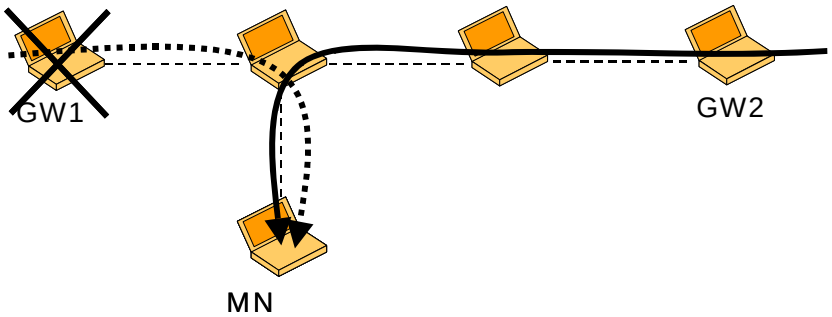

Figure 48: topology for gateway failover

Figure 49 illustrates the relation between the handover latency and the number of BUs sent. It is worth noting that for each handover, one only BU is necessary to register the new CoA. This is because MID messages are used to proactively set up routes to the new registered CoA. The handover latency is determined only by the time required by OLSR to establish the loss of connectivity toward the gateway. The movement detection algorithm does not introduce any other latency.

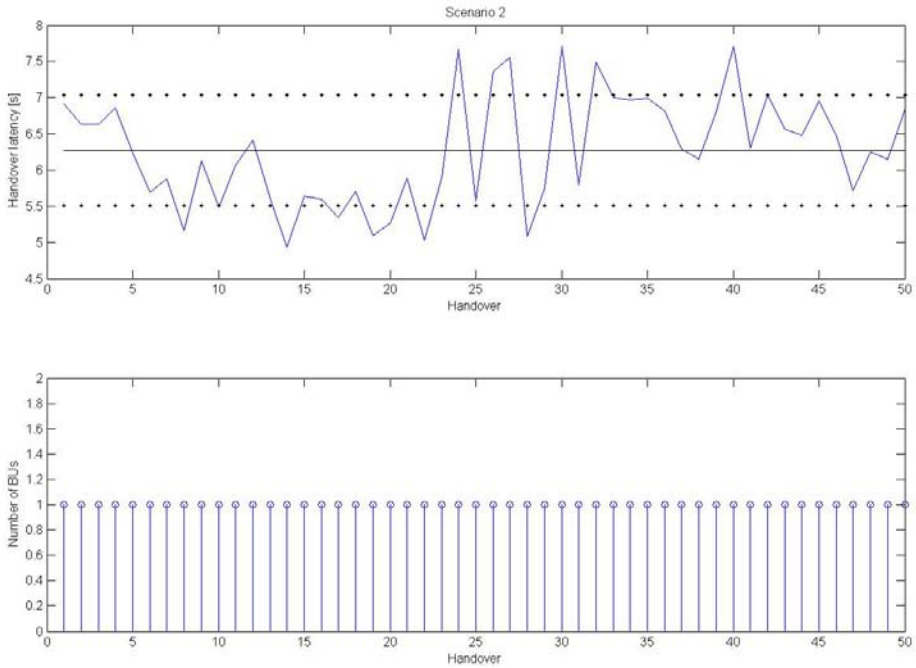

Figure 49: handover latency during gateway failover

As you can see, the introduced modifications of MIPv6/OLSR guarantee upper layer sessions maintenance and the (eventual) downlink path optimization in all considered scenarios. Additionally, the introduction of MIPv6 does not affect hand-off latency, which is still determined by routing protocol (without considering the exponential back-off algorithm), in particular by the routing protocol message emission intervals (PA, Hello, MID) and hysteresis mechanism.

4.2 MANET-NEMO

Figure 50 shows two examples of how NEMO and MANET can be used together. The simplest option is to have a moving network providing WAN connectivity to a MANET, as in Figure 50-A. In the pictured scenario, the WAN interface of the MANET gateway is connected to the on-board LAN of the NEMO Mobile Router. However, the MANET gateway could also be co-located with the MR. The result of this scenario is that the stub MANET benefits from mobile connectivity to the tactical IPv6 backbone.

Another interesting option is to use a MANET, made up of soldiers or other vehicles, as the access medium for a moving network as shown in Figure 50-B. In this case, the MR is equipped with a WAN interface running a MANET unicast routing protocol, such as OLSR. It is also possible for the MR to connect as an attached network to a MANET node. NEMO support allows the vehicle to transparently move from the MANET to an infrastructure-based access (e.g. HF/VHF, satellite), or vice versa.

Using mobility emulation, the scenario shown in Figure 50-A has been successfully tested by IT in the laboratory using currently-available NEMO implementations (NEPL for Linux and experimental Cisco IOS versions) and Unik OLSR. This scenario is one of the key mobility concepts to be demonstrated during the IT national demonstration of INSC Phase II.

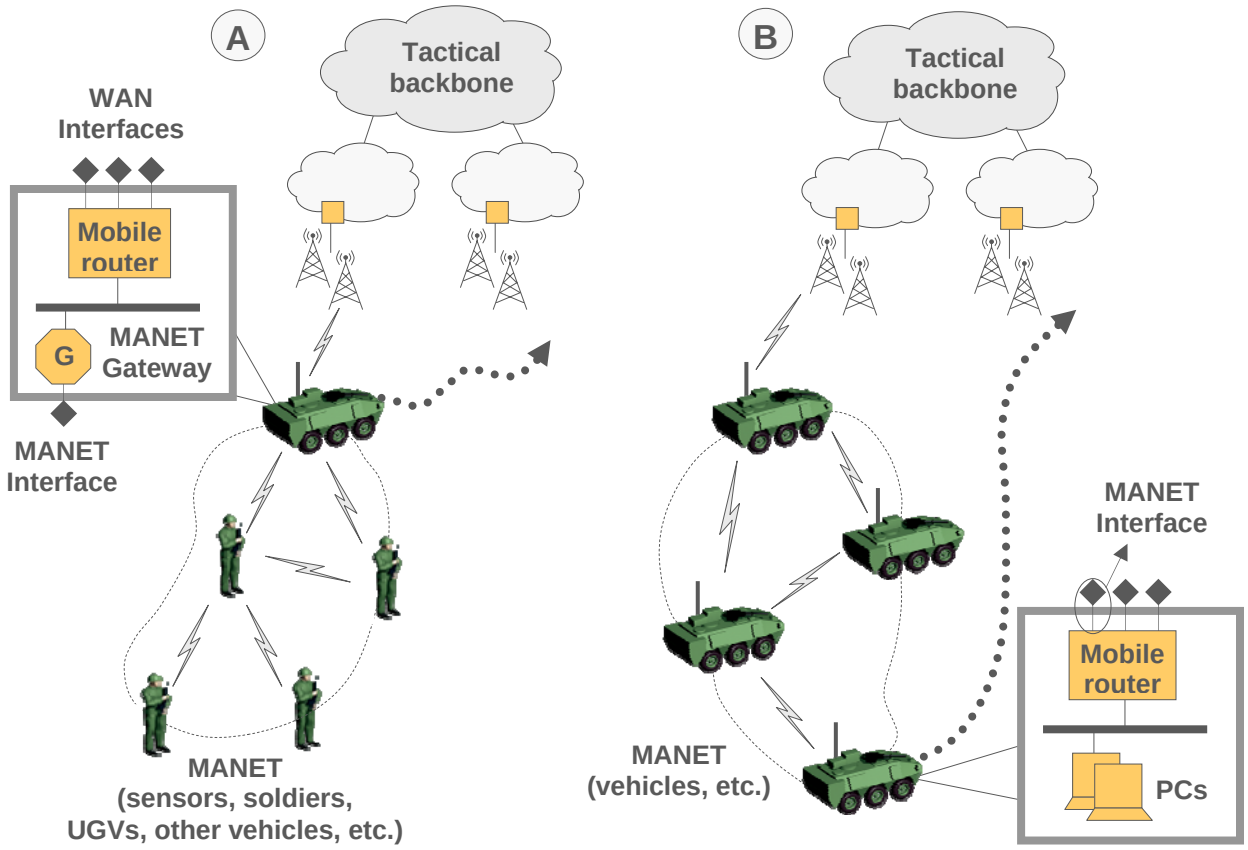

Figure 50: Combined usage of NEMO and MANET

5 Exploitation and Transition

5.1 IETF Transitions

The US has been a significant participant within the Internet Engineering Task Force (IETF), the primary Internet technology standards body. Mr. Joseph Macker, the Task 3 Task Leader, presently serves as a chairman of the Mobile Ad Hoc Networking (MANET) Working Group (WG). The MANET WG is tasked to foster the development of future routing standards for mobile, wireless Internet segments. The MANET WG has progressed a number of mobile routing protocol open specifications to EXPERIMENTAL RFC status (see http://www.ietf.org). Task 3 members have been investigating, and in some cases developing, implementations of these protocols. The MANET WG was also re-chartered during the Phase II timeframe of INSC and is working on a set of follow-on efforts to standardize two MANET unicast routing protocols and simplified multicast forwarding in MANET environments. One of the key focuses is to more carefully consider and support IPv6 functionality within newer

protocols. The development and evolution of Simplified Multicast Forwarding (SMF) for MANET also took a step forward in 2005 with the initial release of a draft specification. Some input from Task 3-related testing has contributed to the development of the early design specifications for these protocols. NRL is the lead editor of the draft specification, and CRC has also contributed to the document. Task 3 also has plans to perform more final testing of SMF within the INSC II testbed. In addition to the MANET WG, Mr. Macker also serves on the design team effort within the IETF looking at MANET extensions to the OSPFv3 protocol. The design team, consisting of other researchers and industry participants, is making progress, and Task 3 has tested prototype code based upon this work. A key point of this work is that it directly addresses an extension for OSPFv3 [5], which is the IPv6 version of OSPF [4]. Additionally, a new working group has recently formed to further investigate auto-configuration within MANET. This group will also focus on IPv6 solutions. Other Task 3 participants are following closely the IETF developments of Hierarchical Mobile IPv6 (HMIPv6) [61], NEMO, IPSec, and Mobile IPv6 and reporting to Task 3 on pertinent issues relating to schedule and risk.

5.2 Related Field Tests and Experiments

5.2.1 German Field Trials

Germany performed many field trials in military training areas during INSC. Within these field trials, MANET technology often played an important role. Consequently, different technologies investigated by Task 3 have been used, such as various OLSR implementations and SMF-based MANET multicasting capabilities. The following describes three field trials performed during INSC Phase II, which involved MANET technology as a substantial part of the trial.

Within the INSC architecture, the concept of a black WAN has been specified, which means establishing MANET networks not only in the red CLAN domain, but also in the black WAN domain. This concept has been successfully demonstrated in one of Germany's field trials during INSC Phase II. Putting MANETs in the black WAN has mainly been motivated due to security aspects. MANETs are usually built on wireless links, which are easier to eavesdrop and access than wired links. Therefore, appropriate security solutions need to be integrated. The German approach within INSC Phase II has been to run IPSec over the MANET network, and thereby secure all traffic sent via a MANET on the network level. This has been realized by putting all applications and services behind a MANET node on its HNA interface. The traffic destined to or originated from this HNA interface is then protected by IPSec.

The INSC security task specified a mechanism for an automatic discovery of IPSec gateways, namely the IPSec Discovery Protocol (IDP). IDP exchanges control messages between all deployed IPSec gateways using multicast. Therefore, black MANETs need multicast support to function as a part of the INSC infrastructure. This IP multicast functionality has been provided by the Simple Multicast Forwarding (SMF) mechanism, and IDP has been shown running successfully over black MANETs.

In many military scenarios, MANETs need to be connected to a remote headquarters. Since there is often no existing infrastructure in place for setting up this connection, mobile satellite links are one suitable method for creating this connection. In one ongoing field trial scenario, several MANET nodes have interfaces to satellite networks, so there are multiple gateways. A QoS-based gateway selection process is done on the MANET nodes to select a gateway using metrics from their WAN connections. The signaling to support the announcement of these metrics has been implemented as new OLSR message type. This demonstration scenario is still ongoing.

Additional German field trials were carried out to test the Linux NEMO implementation. These tests used WLAN cards with external antennas as shown in Figure 51, using multiple access points with like SSIDs, such that the nodes would automatically connect to the foreign access point when they left their home network. The trials verified the correct operation of the NEMO implementation in the field, including nested NEMO operation.

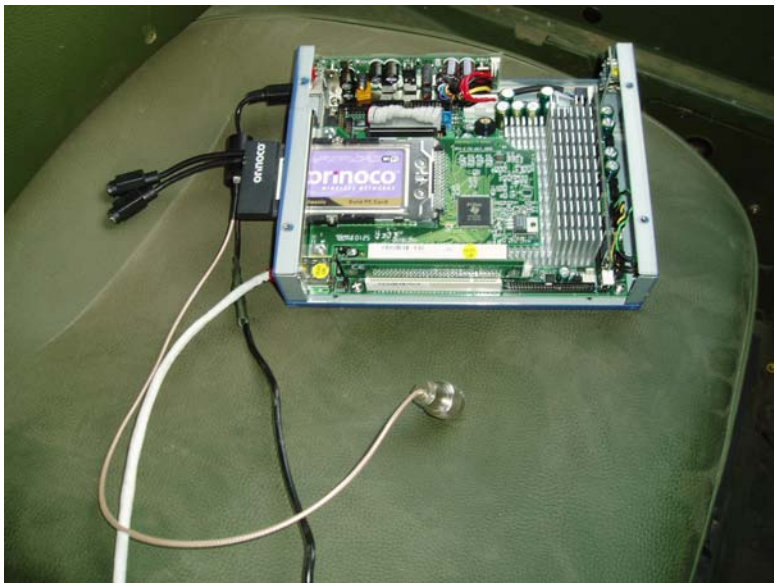

Figure 51: NEMO mobile router based on Linux

In 2005 and 2006, several weeks of field tests have been carried out at a German army training area to test MFP and WNet. The nodes were installed in military trucks, and vehicle-mounted WLAN antennas and external GPS sensors were attached. The field tests confirmed the functionality of the MFP protocol in real-life scenarios, and showed performance results comparable to those attained using emulation, but with higher average packet error rates likely resulting from small scale fading effects. Applications, including VoIP, were run over this network.

5.2.2 Battle Griffin Military Exercise

Exercise Battle Griffin 05 took place in Norway between February 21 and March 11, 2005. This national exercise included involvement from allied nations with 15 participating countries and a total of 14,000 personnel. The main topics for the exercise

were peacekeeping and peace enabling missions in an ethnic, unstable region with terrorist elements trying to further destabilize the situation.

During the exercise, a demonstration of MANET was conducted by the Norwegian Defence Research Establishment (FFI) and the Norwegian Army Transformation and Doctrine Command with support from the 2nd battalion of the Norwegian mechanized infantry brigade “Brig N”.

One platoon from 2nd Battalion was equipped with an ad-hoc radio system in 3 armored fighting vehicles (CV9030N) and on 4 soldiers dismounting from one of the CV90s. In addition, the system was installed in a mobile headquarters and in 3 other vehicles. During the demonstration, the platoon did a traditional recon mission with the infantry soldiers dismounting from the armored vehicles to investigate an area containing suspected hostile elements. The headquarters could, via a battlefield management system, follow the positions of the soldiers and vehicles, send messages, conduct command and control, and receive pictures and videos from the soldiers and vehicles. Figure 52 shows the topology.

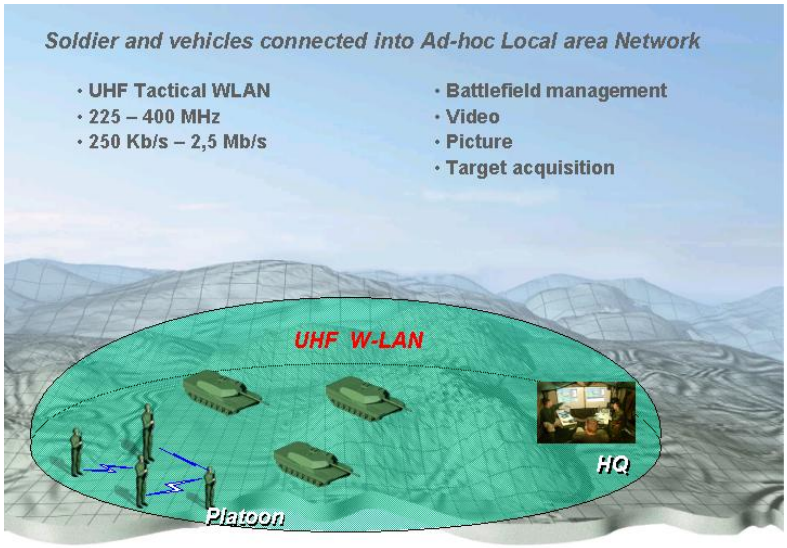

Figure 52: Battle Griffin Exercise

The headquarters was connected to a nationwide network and demonstrated information flowing from the soldiers through the MANET to an operational headquarters located 50 km away. A technical proof-of-concept test of adding a vehicle with SATCOM capacity to the ad-hoc network and using SATCOM to link the ad-hoc network to headquarters was also done

The radio system used for these field trials was developed by Kongsberg and utilizes a modified IEEE 802.11 system, converted to use the UHF band of 250-400MHz and rate-scaled down to ¼ the bit rate and bandwidth. More information about this system can be found in [62]. The radio system used Unik OLSR as the MANET routing protocol.

The field trials showed that saturating the links with traffic did impact the behavior of OLSR. A simple QoS-model was implemented where all OLSR traffic got its own high priority queue. It is, however, clear that priority handling must also be supported at layer 2 to fully ensure proper behavior of the OLSR protocol.

The demonstrations and experiments conducted during this exercise also point to the importance of setting the correct parameters across the layers. For example, timeouts in the different applications must be long enough to allow the network to reorganize itself when the topology changes. The OLSR parameters must also be adjusted based on types of operations and what mobility behavior the military units have. The OLSR parameter settings, coupled with long buffer space in the radios, lead to unwanted short-lived routing loops during the experiments and during controlled lab testing done after the fact.

The demonstration got good reception from the military personnel at the exercise. The ability to perform an operation without spending any time to configure or set up a network was the prime “selling point”. Showing what kinds of applications this network can support, such as a battlefield management system with multimedia capabilities, was also a factor in helping the military personnel understand the value of MANET technology.

5.2.3 French Exploitation and Transition

For several years, the concepts of “battlefield numerisation” and “Network Centric Warfare” (NCW) have made information control a determining stake for the armed forces. NCW doctrine integrates all the tactical components: soldiers, Unmanned Ground Vehicles (UGV), Unmanned Aerial Vehicles (UAV), tactical vehicles, command vehicles, tanks, etc. This concept requires a mesh network architecture, adapting automatically to variable topologies. Such a network performs autoconfiguration, and dynamic routing. It detects the presence of a new node, the absence of another one, and supports node mobility. Networks meeting, wholly or partly, these requirements are under development in the civil world in the form of MANETs.

FR performed urban field experiments at CELAR inside and outside buildings, with pedestrian mobility and MANET nodes in vehicles. The radios used for these experiments were WLAN (802.11b), Bluetooth, Hiperlan1, and a specific military MMW 40 GHz WLAN. The applications used in unicast IPv6 were whiteboard, chat, and video streaming. Additionally, multicast video streaming and VoIP were done in IPv4. France also plans to have a demonstration for military personnel at CELAR on September 2006 demonstrating NEMO and MANET technologies investigated by Task 3.

MANETs are autonomous, self-configuring and self-adaptive networks. Moreover, they adapt themselves to dynamic, random and rapidly changing multi-hop topologies. They have the ability to be deployed rapidly and without any preexisting infrastructure, and are therefore excellent candidates for intelligent transportation systems and military tactical networks, where such capabilities are essential.

Military requirements and constraints make MANET pertinent at the level below the Brigade echelon. New French projects like Operational Aeroterrestrial Bubble (BOA), Future Soldier System (FELIN), Software Defined Radio (SDR), High Data Rate IP Radio (RHD-IP) and other projects in this area could be impacted by these studies.

5.2.4 UK Forward Depth Deployed Sensor (FDDS) Trial

Under UK Ministry of Defence (MOD) funding, QinetiQ developed the concept of a Forward Depth Deployed Sensor (FDDS) network which requires the deployment of small, expendable nodes into areas of interest, able to detect, track and classify targets of interest. These nodes comprise a selection of acoustic sensors, an ability to determine location and orientation, communications between the nodes to form a local, unattended MANET and communications from the MANET back to a user in a remote location.

For the local communications hardware, a commercial product known as Crossbow Motes was taken and adapted to fit the program requirements. In particular, its range and data rates were increased through a number of bespoke improvements to the basic Crossbow design. The software environment used for the local communications solution was a free-to-use, open source development environment called TinyOS, which is targeted specifically at embedded, networked, sensor platforms. A reactive MANET protocol known as TinyAODV (a non-IP embedded variant of AODV) was chosen to provide the MANET capabilities. This type of protocol does not need to continuously send out control messages to ascertain the topology of the network. In addition, a modification was implemented to stop the routes that the protocol generated from being timed out when they were no longer in use. Given the nature of a sensor network, i.e. inactive for long periods of time and only needing to cope with topology events as a result of a node failure, both of these features meant that scarce power and bandwidth would be used more efficiently with little detrimental effect to the performance of the network.

Field trials were conducted from February 2005 to September 2005. Basic trials of the overall sensor package were conducted at QinetiQ Malvern and QinetiQ Pershore while the majority of the trials involving armored vehicles acting as targets were conducted on various areas of Salisbury Plain, a UK MOD training and exercise ground (see Figure 53). A week of successful field demonstrations was also given to the UK MOD customer also at Salisbury Plain in October 2005.

Figure 53: UK FDDS Trial

6 Conclusions

6.1 Dynamic, Wireless Routing

Mobile Ad hoc Network (MANET) technology is useful for supporting military network regions requiring self-organization, mesh operation, and possible high mobility. Since Phase I of INSC, advancements have occurred in both performance extensions and IPv6 support within basic unicast MANET routing. Some existing MANET unicast routing protocols are relatively mature including the Optimized Link State Routing (OLSR) Protocol and the Ad-hoc On Demand Distance Vector (AODV) Protocol, but newer designs continue to evolve within the IETF (e.g., MANET-OSPF, OLSRv2, DYMO [63]). These MANET protocols support both IPv4 and IPv6 operations.

Different MANET protocols have different performance behaviors, and while a subset of 2 or 3 may cover most military scenarios, there is no “one size fits all” design at present. The appropriateness of different solutions has been shown to be related to the intended operational scenarios, applications, and platform requirements (e.g., proactive vs. reactive, vehicular vs. manpack, convoy vs. cluster at deployed HQ, local vs. non-local communications). Additionally, within INSC some MANET implementations and concepts were discovered to be more mature than others.

Newer MANET multicast routing was examined within INSC Phase II and work is now evolving within the standards community as well. Simplified Multicast Forwarding (SMF) is a prime example of an approach that can support improved group communication operations in localized highly mobile routing areas. INSC Phase II demonstrated the use of various test traffic and applications over SMF including:

streaming video, VoIP, mobile multicast chat, file transfer. This technology is also supporting improvement in MANET and mobile technology autoconfiguration techniques. Several connected dominating set (CDS) algorithms for flooding overhead reduction were investigated by T3 within SMF, providing a range of solutions with differing levels of overhead, distributed operation, and mobility robustness. In addition to SMF, group based multicast (e.g. MOLSR, MFP) was also examined as an alternate MANET multicasting strategy. With these protocols, multicast transmissions are confined to only those nodes on the forwarding path of the multicast group subscribers (which may change over time). This may reduce the amount of loading placed on the network compared to flooding in certain topologies when the number of subscribers is much smaller than the total number of nodes in the network. However, it is unclear how much performance may be gained, given the added complexity of maintaining subscriber and forwarding trees under mobility for each multicast group in the network.

MANET autoconfiguration has also been an important work item within INSC Phase II and the results will be of value to the operational community in order to both reduce the time needed to deploy their tactical networks and reduce the amount of skilled pre-configuration these networks would otherwise require. Stateful (DHCP) and stateless (distributed router advertisements) methods for IP address and default gateway autoconfiguration were investigated. In addition, a distributed DNS system known as DMDNS was designed and tested within INSC to overcome mobility issues faced by standard DNS within MANETs.

6.2 Edge Mobility

Mobile IPv6 and potential extensions (hierarchical MIP) were investigated by Task 3. MIPv6 implementations have become more mature and have become more widely available, but the inclusion of IPSec integration into the protocols is still evolving. Standard specifications for Hierarchical MIP have advanced more slowly than anticipated at the beginning of INSC Phase II and have been studied less during this time period.

Network Mobility (NEMO) provides newer technology enhancement for aggregate prefix mobility. As a newer technology extension of MIPv6 concepts, NEMO may provide more relevant military support for larger platform and network mobility across and within WAN architectures. Task 3 investigated this technology's basic modes and some extended operational modes (e.g., NEMO nesting). Basic NEMO is presently functional, but implementations are still not stable (more testing is recommended). At present, software bugs and missing protocol features have been discovered by Task 3 researchers. The NEMO nesting function (multiple NEMO tunnels) has been shown to work, but there is little experience with the performance impact of current solutions. There are also important architectural issues resulting from additional encapsulation with each nesting level.

There may be architectural and scenario-specific issues related to the use and distribution of home agent functionality. For instance, in a tactical scenario, the home network provides a single point of failure. Further investigation is needed in this area.

Additionally, tests performed by Task 3 showed that current protocols may not be sufficient for fast handoff latency scenarios without additional engineering attention. Finally, INSC Phase II also demonstrated the ability to autoconfigure the MIPv6/NEMO Home Agents.

6.3 Other Technologies

Task 3 also demonstrated significant advancements in both MIPv6 and NEMO operation by examining the potential for integration within an operation MANET network.

Additionally, there are some technologies investigated which had an impact in both MANET and edge mobility. Cross layering is becoming more mature, and several science and technology projects, including INSC, have begun to demonstrate the value of such design approaches.

7 Operational and Future Work Recommendations

7.1 Dynamic, Wireless Routing

Task3 recommends that MANET solutions be considered for tactical edge routing scenarios and that prior to any deployment additional technical efforts should address design integration with evolving tactical wireless technologies. Each wireless technology and MAC layer will present different opportunities, challenges, and performance issues. INSC has studied a variety of MANET unicast routing solutions evolving within the Internet open standards community. Proactive MANET routing approaches, such as OLSR and MANET-OSPF, are recommended for consideration when more constant communication support is needed and robustness is desired, especially intra-vehicular. The overhead for these protocols can be better engineered and is more predictable under a variety of traffic and mobility conditions. Reactive protocols, such as AODV or DYMO, may be useful when energy constraints are a paramount concern and traffic flows are sparse (e.g., sensor networks). All MANET approaches studied support localized routing under node mobility in addition to the ability to advertise prefixes or additional subnetworks attached to a node (e.g., vehicular LANs, etc).

T3 recommends that optimized wireless multicast forwarding solutions, such as Simplified Multicast Forwarding (SMF), be integrated into future tactical edge network systems. SMF can provide efficient delivery of application data within a MANET routing area. This can provide increased efficiency for a variety of applications (e.g., situational awareness, multicast VoIP, video streaming, chat, etc). T3 demonstrated a variety of multicast IP application working within prototype mobile networks using SMF. T3 also recommends that further work be done in the area of group-based multicast to investigate the robustness of such protocols and determine whether significant performance gains can be made compared to flooding techniques such as SMF.

T3 recommends that MANET solutions initially be considered for stub network deployments to support the tactical edge. Future transit network applications and more complex gateway interactions can be supported, but would require more study

concerning the scalability of current approaches and considering scenario specific requirements. MANETs should also be planned for deployment with consideration for appropriate hierarchies, multiple MANET routing areas rather than larger flat routing areas.

Further work on MANET autoconfiguration is recommended and early work by T3 shows promise in the areas of MANET/edge integration and the use of SMF for supporting autoconfiguration and discovery services. Competing techniques should be compared and recommended for specific operational scenarios. This work should contribute to the emerging IETF MANET autoconfiguration WG standardization efforts in order to achieve widespread acceptance and vendor compatibility in future Coalition operations. Further development of DMDNS is recommended to resolve the outstanding technical issue of interfacing with standard DNS and to fully assess its scaling qualities.

If MANET devices are deployed primarily as routers, they may be configured to use unnumbered or link local addresses (IPv6) to ease the burden of configuration. In this case, the MANET routers would serve to support and advertise attached prefix addresses and would operate similar to fixed infrastructure IP routing configurations. One issue here is that it is recommended that unique MAC or 64 bit IEEE EUIDs be deployed so that complex duplicate address detection (DAD) schemes can be avoided.

7.2 Edge Mobility

Edge Mobility Technology enhancements (e.g., NEMO and MIPv6) provide benefit in some example tactical use case scenarios developed by T3. If devices or platforms are required to maintain their global IP addresses or prefixes when mobile across an infrastructure, then NEMO and MIPv6 can provide benefits. NEMO provides additional benefits when blocks of addresses are expected to move as whole networks (e.g., ships, vehicular LANs, etc). If low-latency connection handoff scenarios are important, edge mobility solutions need additional engineering attention prior to deployment consideration. MIPv6 and NEMO can directly support the retention of active network connections since the endpoint addressing does not change. Further studies are recommended to be conducted to examine application and transport specific performance in this area.

NEMO handles aggregate network prefixes mobility (platform mobility scenarios). This is useful for various use cases given mobility within a larger military backbone network and we recommend this be considered as a possible solution for those cases. This may have a side benefit of improving overall network management since home addresses can remain static. If mobility is expected to be largely localized within a topology a routing protocol or MANET solution may be a better choice. Since we expect both localized and macromobility situations to occur, we recommend both technologies be considered for deployment.

7.3 Other

It should be noted that while T3's work was done mainly at Layer 3 (IP), the technologies and algorithms can also be applied at Layer 2 if desired. Layer 3 has a heterogeneous and cost value since it is somewhat technology-agnostic. It is also possible to combine the two solution types. T3 recommends more consideration be given to cross layer performance to improve efficiency performance and delay. One example is the use of lower layer interface information to improve neighbor link status, activation, and deactivation.

T3 recommends that future work address issues in supporting specific scenarios and examine particular protocol extensions and optimizations as appropriate to support architectural and mission needs (e.g., EMCON nodes). We also recommend further attention be paid to security requirements in future work. At present, we recommend that particular security solutions are scenario dependent.

ANNEX A: RELATED ACTIVITIES

MANET Supervision

A MANET made up of 18 nodes, running OLSR and using WLAN radios, was deployed at CELAR. Work described below was done with the goal of supervising this testbed. A supervisor is a software component installed on a machine which allows it to control and manage elements of the network. The software used for MANET supervision is the SNMPc Enterprise Edition version 6.0.5 of Manor house Rock'n'roll.

SNMPc collects information about network equipment via SNMP agents. For the CELAR MANET network, only four Linux laptops were equipped with an SNMP agent. The other nodes, INRIA experimental routers and Compaq PDAs, have a reduced Linux environment and could not be equipped with an SNMP agent. The supervision of these INRIA experimental routers is done via their answers to ICMP messages transmitted by the supervisor software, in order to determine their operating condition.

A layout of the MANET network was established by the supervisor, thanks to SNMPc, which integrates an automatic equipment discovery agent. The supervisor automatically discovers the equipment equipped with SNMP agents, and with knowledge, also of the other equipment (INRIA routers) responding to the ICMP ping.

The operating condition of each piece of equipment is displayed in the events window, with the associated date and hour. One can use this information to determine, for example, at what time equipment a piece of equipment was unreachable, and when it became reachable again. For further information, please see [64].

OLSR QoS

The goal of this work was to enhance the OLSR protocol in order to support QoS routing while taking interference into account. The QoS architecture requires five components to support QoS management in a MANET. These five building blocks are illustrated in Figure 54. A cross-layer QoS model was used to support adaptivity and optimization across multiple layers of the network stack.

Figure 54: QoS Architecture

To provide a simple solution, we define three QoS classes. For user flows, *Class* 1 is the highest priority, and should be used for flows having a high importance for the user or requiring low delay (e.g. VoIP). *Class* 2 is suitable for flows requiring high data rates (e.g. video streaming). *Class* 3 is the default category, and corresponds to a best effort (BE) service. Flows having delay constraints are processed before flows having bandwidth constraints, but after control flows such as OLSR packets.

In order to select the route meeting the bandwidth required, the routing protocol must know the bandwidth locally available at each node. QoS signaling is introduced for that purpose. The chosen solution generates the same number of retransmissions per message broadcast in the MANET as native OLSR. QoS routing selects the shortest route (minimum hop count) providing the requested bandwidth. If several routes exist, the route with the widest available bandwidth is chosen. Such an algorithm is called the widest shortest path algorithm. The routing algorithm differs according to the class of the flow.

The purpose of QoS admission control is to accept a new QoS flow if and only if both of the following conditions are met: the requested QoS level can be met (all nodes on the path are able to provide the requested bandwidth), and the QoS of already-accepted QoS flows is not compromised by the acceptance of the new flow (all nodes in the interference area of a node on the path have enough bandwidth). The admission control is performed locally by the source, and it is done periodically in order to optimize resource utilization. For further information, please see the reference whitepapers [65], [66], and [67].

OLSR Security

The goal of this work was to study security issues in OLSR, provide a detailed security architecture for the French MANET demonstrator network, and quantify the behavior of this security architecture. A theoretical study identified five different OLSR attack

methods: the incorrect control message generation attack, the replay attack, the relay attack, the bad data traffic relaying attack, and the bad control traffic relaying attack. All these attacks may have important consequences on network connectivity.

In a MANET, a node is said to be compromised if it does not process and emit control traffic in accordance with the routing protocol specifications, or if it does not perform the implied data packet forwarding correctly. Under the assumption that there are no compromised nodes in the network, a cryptographically-capable MANET can counter all identified attacks except the relay attack using signature and time-stamps mechanisms. Doing so will prevent intruder nodes from joining the network. The relay attack can be countered in most situations when the network nodes know their own location.

The security architecture of the demonstrator uses a shared key with symmetric cryptography. As in the theoretical study, our design security architecture is based on the use of signatures and time stamps. In the demonstrator, we therefore implement the HMAC authentication algorithm (with MD5 hashing function) for signatures. This technique uses a symmetric shared key. In the theoretical study, we have proposed to authenticate Hello and TC control messages by using signatures. However, there exist other messages which carry routing information in OLSR: MID and HNA messages. Signing HNA messages is mandatory to protect the network against dissemination of wrong accessibility information. Similarly, when the network includes nodes with multiple interfaces, MID messages are used not only to get the correct routes to all the network interfaces, but also to correctly compute the MPR set. Thus, signing MID is also necessary to prevent attacks. In the demonstrator, we thus sign Hello, TC, MID and HNA messages.

The time stamps are simply the times given by a node's internal clock. A strict synchronization of clocks is not necessary, since the time stamp is used to complete the protection already offered by the Message Sequence Number and the duplicate set. In fact, messages that are already in the duplicate set are silently dropped.

As already stated, attacks in which there are compromised nodes are not included in this work. We use four scenarios to validate the proposed security architecture. There is no attack in the first scenario. The three other presented scenarios correspond mainly to attacks related in the theoretical study as incorrect control message generation attacks. We plan to qualify the performance of the network under these attacks based on whether the attack was successful, as well as the cost for the network to implement the specified security architecture. In order to check the proper functionality of the specification and implementation, several validation tests were performed in simulation using the secure version of OLSR. In addition, because the security architecture proposed does not modify the parts of the implementation related to operating system interaction (setting routes, sending and receiving messages, etc.), these tests would actually validate most of the changes for security. For further information, please see [68] and [69].

Mobile IPv6 Between Heterogeneous Networks

France performed tests with Mobile IPv6 on networks with a mix of Ethernet and Bluetooth networks. The topology used for these experiments is shown in Figure 55.

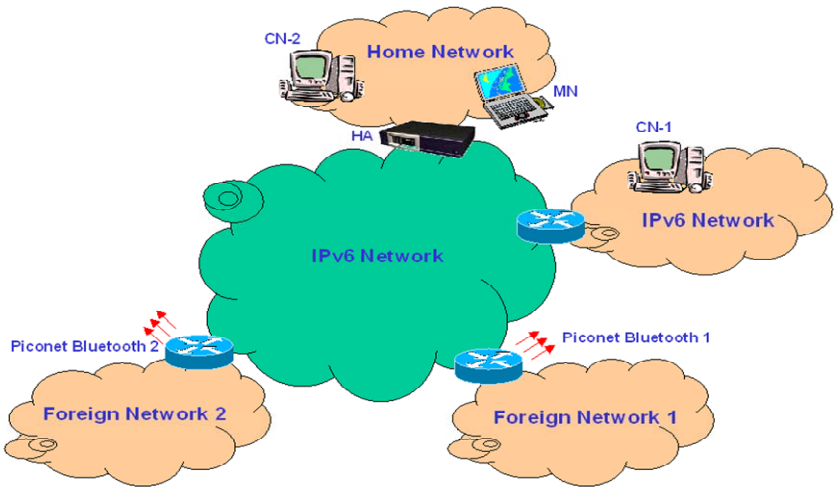

Figure 55: Heterogeneous MIPv6 topology

The experiments of heterogeneous mobility carried out at CELAR showed some interoperability problems. These problems can be partially avoided by manually modifying the Neighbor Discovery Protocol entries on machines wishing to contact the MN, but the user does not always have the possibility of doing that. No problems were experienced when moving from the fixed Ethernet network to the Bluetooth wireless networks. For further information, please see [70].

ANNEX B: GLOSSARY

AAA	Authentication, Authorization and Accounting
AODV	Ad Hoc On-Demand Distance Vector routing protocol
AP	Access Point
AR	Access Router
AS	Autonomous System
AVP	Attribute-Value Pair
BA	Binding Acknowledgement
BCS	Best CoA Selection algorithm
BGP	Border Gateway Protocol
BU	Binding Update
C3	Consultation, Command and Control
CA	Canada
CDS	Connected Dominating Set
CELAR	Centre d'Electronique de l'ARmement (FR)
CF	Classical Flooding
CLAN	Coalition LAN
CN	Correspondent Node
CoA	Care-of Address
CRC	Communications Research Centre Canada
CSMA/CA	Carrier Sensed Medium Access Collision Avoidance
DAD	Duplicate Address Detection
DDNS	Dynamic DNS
DHAAD	Dynamic Home Agent Address Discovery
DHCP	Dynamic Host Configuration Protocol
DMDNS	Distributed MANET DNS
DNS	Domain Name Service
DPD	Duplicate Packet Detection
DS	Dominating Set
DYMO	Dynamic MANET On Demand routing protocol
E-CDS	Essential Connected Dominating Set
EAP	Extensible Authentication Protocol
EGP	External Gateway Protocol
EMCON	Emission Control
ETSI	European Telecommunications Standards Institute
EUI-64	64-bit Extended Unique Identifier
FDDS	Forward Depth Deployed Sensors
FEC	Forward Error Correction
FFI	Norwegian Defence Research Establishment
FGAN	Forschungsgesellschaft für Angewandte Naturwissenschaften (GE)
FR	France
FTP	File Transfer Protocol
GE	Germany
GPS	Global Positioning System
GTNETS	Georgia Tech Network Simulator

HA	Home Agent
HMIPv6	Hierarchical Mobile IPv6
HNA	Host and Network Association
HQ	Headquarters
ICMP	Internet Control Message Protocol
IDP	IPSec Discovery Protocol
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IGP	Internal Gateway Protocol
IKE	Internet Key Exchange
INRIA	Institut National de Recherche en Informatique et Automatique (FR)
INSC	Interoperable Network for Secure Communications
IOS	Cisco Internet Operating System
IP	Internet Protocol
IPSec	IP Security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IT	Italy
LAN	Local Area Network
LFN	Local Fixed Node
LNE	Large Network Emulator
LOS	Line of Sight
LSA	Link State Advertisement
MAC	Media Access Control
MAGMA	Multicast and Anycast Group Membership
MANET	Mobile Ad Hoc Network
MANET-OSPF	MANET Extensions to OSPF
MCDS	Minimum Connected Dominating Set
MDP	Multicast Dissemination Protocol
MDR	Manet Designated Router
MFP	Manet Forwarding Protocol
MGEN	Multi Generator
MID	Multiple Interface Declaration
MIPL	MIPv6 for Linux
MIPv6	Mobile IPv6
MLD	Multicast Listener Discovery
MN	Mobile Node (MIPv6)
MNE	Mobile Network Emulator
MOD	UK Ministry of Defence
MOLSR	Multicast OLSR
MPR	Multipoint Relay
MR	Mobile Router
MS-CHAP	Microsoft Challenge-Handshake Authentication Protocol
MTU	Maximum Transmission Unit
NACK	Negative Acknowledgement
NAS	Network Access Server

NATO	North Atlantic Treaty Organization
NC3A	NATO C3 Agency
NCW	Network-Centric Warfare
NEMO	Network Mobility
NEPL	NEMO Platform for Linux
NL	Netherlands
NO	Norway
NORM	Nack Oriented Reliable Multicast
NRL	US Naval Research Laboratory
NS-MPR	Non-Source Specific MPR
NUD	Neighbor Unreachability Detection
OLSR	Optimized Link State Routing protocol
OLSRv2	OLSR Version 2
ONR	US Office of Naval Research
OSPF	Open Shortest Path First
P2P	Peer-to-Peer
PA	Prefix Advertisement
PDA	Personal Digital Assistant
PEAP	Protected EAP
PIM	Protocol Independent Multicast
PIM-DM	PIM-Dense Mode
PIM-SM	PIM-Sparse Mode
PO	Participating Organization
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
RADV	Router Advertisement
RFC	Request For Comments
RIP	Routing Information Protocol
RR	Resource Record
RSH	Remote Shell
RTS/CTS	Request To Send/Clear To Send
RTT	Round Trip Time
SMF	Simplified Multicast Forwarding
SNMP	Simple Network Management Protocol
SNP	Service Negotiation Proxy
SSH	Secure Shell
SSID	Service Set Identifier
T3	Task 3 (Mobility Task)
TC	Topology Control
TCP	Transmission Control Protocol
TLS	Transmission Layer Security
TLV	Type Length Value
TTL	Time To Live
UAV	Unmanned Aerial Vehicle
UDP	User Datagram Protocol
UGS	Unattended Ground Sensors

UGV	Unmanned Ground Vehicle
UK	United Kingdom
US	United States of America
VLAN	Virtual LAN
VoIP	Voice over IP
WAN	Wide Area Network
WG	Working Group (IETF)
WIGMP	Wireless IGMP
WLAN	Wireless LAN
WNET	Wireless Network

ANNEX C: REFERENCES

[1] *Task 3 Mobile Networking Technology Assessment and Considerations*, INSC-II/Task3/Task3/D/001, June 2005, http://insc.nodeca.mil.no/.

[2] *Task 6 Final Report*, INSC/Task6/DU/008, December 2003, http://insc.nodeca.mil.no/.

[3] C. Hedrick. *Routing Information Protocol*, RFC 1058, June 1988.

[4] J. Moy. *OSPF Version 2*, RFC 2328, April 1998

[5] R. Coltun, D. Ferguson, J. Moy. *OSPF for IPv6*, RFC 2740, December 1999.

[6] Y. Rekhter, T. Li. *A Border Gateway Protocol 4 (BGP-4)*, RFC 1771, March 1995.

[7] T. Clausen, P. Jacquet. *Optimized Link State Routing Protocol (OLSR)*, RFC 3262, October 2003.

[8] C. Perkins, E. Belding-Royer, S. Das. *Ad hoc On-Demand Distance Vector (AODV) Routing*, RFC 3561, July 2003.

[9] E. Baccelli, T. Clausen, P. Jacquet. *OSPF MPR Extension for Ad Hoc Networks*, draft-baccelli-ospf-mpr-ext-02, March 2006.

[10] J. Macker, et al. *Simplified Multicast Forwarding for MANET*, draft-ietf-manet-smf-02, March 2006.

[11] Joseph P. Macker, William Chao, Jeffery W. Weston. "A Low-Cost, IP-based Mobile Network Emulator", *IEEE MILCOM 2003 Proceedings*, October 2003.

[12] NRL OLSR implementation, http://pf.itd.nrl.navy.mil/olsr/.

[13] The Network Simulator ns-2, http://www.isi.edu/nsnam/ns/.

[14] OPNET Technologies, Inc., http://www.opnet.com/

[15] NRL Multi-Generator (MGEN) software, http://pf.itd.nrl.navy.mil/mgen/.

[16] T. Clausen, C. Dearlove, et al. *The Optimized Link-State Routing Protocol version 2*, draft-ietf-manet-olsrv2-01, March 2006.

[17] CRC OLSR Implementation, http://www.crc.ca/en/html/manetsensor/home/software/software.

[18] Unik OLSR implementation, http://www.olsr.org/.

[19] INRIA OLSR implementation, http://hipercom.inria.fr/olsr/.

[20] Thomas R. Henderson, Phillip A. Spagnolo, Guangyu Pei. *Evaluation of OSPF MANET Extensions*, Boeing Technical Report D950-10897-1, July 2005.

[21] Boeing MANET OSPFv3 implementation, http://hipserver.mct.phantomworks.org/ietf/ospf/.

[22] Quagga Software Routing Suite, http://www.quagga.net/.

[23] Georgia Tech Network Simulator, http://www.ece.gatech.edu/research/labs/MANIACS/GTNetS/.

[24] Tom Henderson, Marcelo Albuquerque, Phil Spagnolo, Jae H. Kim. "Interlayer routing issues for wireless networks", *Proceedings of NRL Cross-Layer Workshop*, June 2004.

[25] Uppsala University AODV Implementation, http://core.it.uu.se/AdHoc/.

[26] *An Experimental Comparison of MANET Unicast and Multicast Routing Protocols*, INSC-II/UK/Task 3/D/001, May 2006.

[27] *Interconnecting OLSR and OSPF*, INSC-II/FR/Task 3/D/005, September 2005.

[28] *MANET Forwarding Protocol (MFP) for Multicast and Unicast Traffic, Specification and Implementation*, INSC-II/GE/Task 3/D/002, March 2006.

[29] Thomas Bachran, Harald H.-J. Bongartz, Alexander Tiderko. "A Framework for Multicast and Quality Based Forwarding in MANETs", *CCN '05: Proceedings of the 3rd IASTED International Conference on Communications and Computer Networks*, ACTA Press, 2005.

[30] NRL SMF implementation, http://pf.itd.nrl.navy.mil/smf/.

[31] S. Ni, Y. Tseng, Y. Chen, J. Sheu. "The Broadcast Storm Problem in Mobile Ad hoc Networks", *Proceedings of MOBICOM 99*, pgs. 151-162, August 1999.

[32] M.R. Garey, D.S. Johnson. *Computers and Intractability: A Guide to the Theory of NP-Completeness*. Freeman and Company, 1979.

[33] J. P. Macker, J. Dean, W. Chao. "Simplified Multicast Forwarding in Mobile Ad Hoc Networks", *IEEE MILCOM 2004 Proceedings*, November 2004.

[34] B. Adamson, C. Bormann, M. Handley, J. Macker. *Negative-acknowledgement (NACK)-Oriented Reliable Multicast (NORM) Protocol*, RFC 3940, November 2004.

[35] J. Macker, W. Dang. *The Multicast Dissemination Protocol (MDP) Framework*, draft-macker-mdp-framework-02 (expired), May 1997.

[36] P. Jacquet, P. Minet, A. Laouiti, L. Viennot, T. Clausen, C. Adjih. *Multicast Optimized Link State Routing*, draft-ietf-manet-olsr-molsr-01 (expired), November 2001.

[37] INRIA MOLSR Implementation, http://hipercom.inria.fr/SMOLSR-MOLSR/.

[38] *Multicast for MANET/OLSR*, INSC/FR/Task6/D/009, July 2003.

[39] *MOLSR and BonePhone experimentations*, INSC-II/FR/Task 3/D/011, May 2006.

[40] D. Estrin, D. Farinacci, A. Helmy, D. Thaler, S. Deering, M. Handley, V. Jacobson, C. Liu, P. Sharma, L. Wei. *Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification*, RFC 2362, June 1998.

[41] A. Adams, J. Nicholas, W. Siadak, *Protocol Independent Multicast-Dense Mode (PIM-DM): Protocol Specification (Revisde)*, RFC 3973, January 2005.

[42] Bill Fenner, Haixiang He, Brian Haberman, Hal Sandick. *IGMP/MLD-based Multicast Forwarding ("IGMP/MLD Proxying")*, draft-ietf-magma-igmp-proxy-06 (expired), April 2004.

[43] Multicast Gateway (MLD_Proxy) software, http://clarinet.u-strasbg.fr/~frey/.

[44] *Simplified Multicast Forwarding Final Report*, INSC-II/CA/Task 3/D/001, May 2006.

[45] *MLD Proxy*, INSC-II/NL/Task 3/D/001, January 2006.

[46] S. Thomson, T. Narten. *IPv6 Stateless Autoconfiguration*, RFC 2462, December 1998.

[47] R. Droms. *Dynamic Host Configuration Protocol*, RFC 2131, March 1997.

[48] R. Droms, J. Bound, B. Volz, T. Lemon, C. Perkins, M. Carney. *Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*, RFC 3315, July 2003.

[49] S. Ruffino, P. Stupar. *Automatic configuration of IPv6 addresses for MANET with multiple gateways*, draft-ruffino-manet-autoconf-multigw-02, February 2006.

[50] Autoconfiguration in IPv6 wireless ad hoc networks software (GWINFO), http://clarinet.u-strasbg.fr/~frey/.

[51] C. Jelger, T. Noel, A. Frey. *Gateway and address autoconfiguration for IPv6 adhoc networks*, draft-jelger-manet-gateway-autoconf-v6-02 (expired), April 2004.

[52] D. Johnson, C. Perkins, J. Arkko. *Mobility Support in IPv6*, RFC 3775, June 2004.

[53] V. Devarapalli, R. Wakikawa, A. Petrescu, P. Thubert. *Network Mobility (NEMO) Basic Support Protocol*, RFC 3963, January 2005.

[54] G. Giaretta, J. Kempf, V. Devarapalli. *Mobile IPv6 bootstrapping in split scenario*, draft-ietf-mip6-bootstrapping-split-02, March 2006.

[55] K. Chowdhury, A. Yegin. *MIP6-bootstrapping via DHCPv6 for the Integrated Scenario*, draft-ietf-mip6-bootstrapping-integrated-dhc-00 (expired), October 2005.

[56] G. Giaretta, I. Guardini, E. Demaria, J. Bournelle, M. Laurent-Maknavicius. *MIPv6 Authorization and Configuration based on EAP*, draft-giaretta-mip6-authorization-eap-03, March 2006.

[57] NEMO Platform for Linux (NEPL), http://www.mobile-ipv6.org/software/.

[58] MIPL Mobile IPv6 for Linux (MIPL), http://www.mobile-ipv6.org/software/.

[59] NEPL-SE NEMO Implementation, http://software.nautilus6.org/NEPL/index.php.

[60] *Report on NEMO Experiments*, INSC-II/Task 3/D/004, March 2006.

[61] H. Soliman, C. Castelluccia, K. El Malki, L. Bellier. *Hierarchical Mobile IPv6 Mobility Management (HMIPv6)*, RFC 4140, August 2005.

[62] Vegard Arneson, Knut Øvsthus, Ole Ingar Bentstuen, Jostein Sander. "Field Trials with IEEE 802.11b-based UHF Tactical Wideband Radio", *IEEE MILCOM 2005 Proceedings*, October 2005.

[63] I. Chakeres, C. Perkins. *Dynamic MANET On-demand (DYMO) Routing*, draft-ietf-manet-dymo-04, March 2006.

[64] *Supervision of Network*, INSC-II/FR/Task 3/D/006, January 2006.

[65] *Quality of Service in MANETs*, INSC-II/FR/Task 3/D/002, January 2006.

[66] *Scalability and Quality of Service Support with OLSR*, INSC-II/FR/Task 3/D/003, January 2006.

[67] *Technical Specifications of QoS Support Platform Implemented on the OLSR Platform*, INSC-II/FR/Task 3/D/004, September 2005.

[68] *Securing the OLSR routing protocol with or without compromised nodes in the network*, INSC-II/FR/Task 3/D/001, May 2005.

[69] *OLSR Security*, INSC-II/FR/Task 3/D/009, January 2006.

[70] *Heterogeneous Ethernet / Bluetooth MobileIPv6 experiments*, INSC-II/FR/Task 3/D/007, January 2006.