# TECHNOLOGIES AND STANDARD APPLICATIONS OF MANEMO IN VEHICULAR NETWORKS

Vijayakranthi Chinthala[1], Manas Kumar Yogi[2]
[1]M.Tech Student, [2]Sr. Assistant Professor
[1]Indur Institute of Engineering and Technology
[2]Ellenki Engineering College
Department of Computer Science and Engineering
Siddipet, India.

***Abstract:*** ***Mobile ad hoc NEMO (MANEMO) is a technology introduced to integrate the capabilities of NEMO and MANET. MANEMO is defined in many ways as "Mobile ad hoc NEMO", "MANET and NEMO", "management of nested NEMO", and "MANET for NEMO". NEMO provides movement transparency to a network, while MANET provides ad hoc routing with neighboring nodes. Several industries such as transportation and the military look for both capabilities in their network systems. MANEMO introduces a new concept known as the wireless fringe stub a cloud of NEMO-capable mobile routers connected by wireless or wired links and a stub at the edge of the Internet, interconnecting various types of devices, which discover each other and form a network in an ad hoc fashion to provide global connectivity to each other. One example of MANEMO networks is a vehicular network. The concept of MANEMO, possible issues, and proposed solutions are presented in this paper.***

***Keywords:*** ***NEMO, MANEMO, Vehicular Networks, VANET, Routers.***

## I. INTRODUCTION

When the network mobility support protocol is widely deployed to vehicles, public transportation, and even personal area networks (PANs), it is expected that the impact on existing network environments would be substantial. Current mobility protocols rely on the availability of well-managed, fixed network infrastructures. From the mobile node point of view, once the node acquires connectivity, it is assured of reach ability and communication to the Internet. However, as network mobility support becomes available, a mobile node no longer assumes the presence of such fixed infrastructures. The mobile node may attach to the Internet through mobile routers providing the Internet connectivity. There is no guarantee that the mobile node always gets reach ability to the Internet over the mobile router since the mobile router is also moving and may lose connectivity to the infrastructure. Since a mobile network provided by a mobile router can be viewed as a regular IPv6 network, the mobile node cannot tell whether it is connected to a mobile network or a fixed network. These causes a major change to the connectivity assumption of the mobile node. Moreover, by nesting mobile routers, multiple wireless hops appear on the path between end nodes. Most wireless communication today consists of the last-one-hop wireless path and the fixed infrastructure.

## II. MANEMO WIRELESS FRINGE STUB

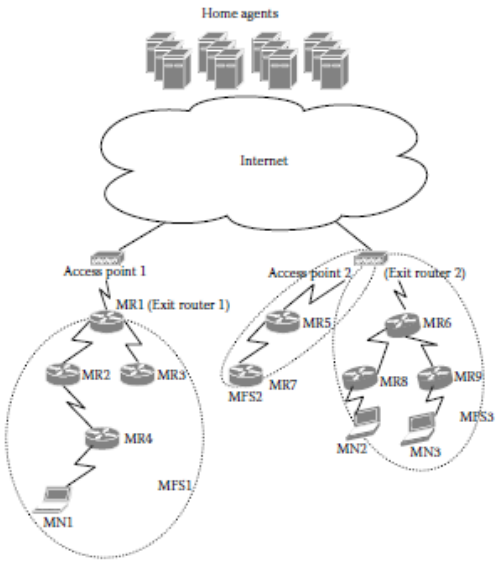


Figure 1: Mobile Fringe Stub

When mobile routers and mobile nodes converge at the edge of the Internet using wireless interfaces, they can form a wireless network cloud. This type of network is called a MANEMO fringe stub (MFS). An MFS is a stub at the edge of the Internet, interconnecting various types of devices, which discover each other and form a network in an ad hoc fashion to provide Internet connectivity to one another. Participants in an MFS are not only mobile routers but also mobile hosts, fixed hosts, and fixed routers. The fixed nodes are located either within one of the mobile networks or within the fixed infrastructure. The exit router is a router that provides Internet connectivity in MFS.

In "Fig. 1", the exit router is either a mobile router connected directly to the Internet (Exit Router1) or a fixed access router

  

supporting MANEMO (Exit Router2).

Multiple exit routers may be available in an MFS, Different types of links are used to form an MFS, including WiFi, Bluetooth, 802.15.4, and meshed wireless technology (802.11s, 802.11 in ad hoc mode, etc.). Exit routers are connected to the infrastructure by wired link, Wi-Fi, Wi-MAX, and cellular technology (LTE, HSDPA, EvDo, GPRS, etc.). An MFS can also be disconnected from the infrastructure. In such a disconnected MFS, mobile routers communicate only with nodes inside the same MFS. Any node which needs Internet connectivity has to select the best exit router toward the Internet. Therefore, it is necessary for mobile nodes to maintain a local topology in the MFS. MANEMO provides the necessary additions to existing protocols (IPv6, NDP, NEMO), for the MFS to find the most suitable exit router for the infrastructure. MANEMO enables basic internal connectivity within the MFS whether the infrastructure is reachable or not.

## III. MANEMO CHARACTERISTICS AND REQUIREMENTS

When we consider MFS and MANEMO, several new features are introduced to the mobility environment. This section presents the characteristics and requirements of MANEMO by comparing existing solutions such as NEMO and MANET.

### A. Supporting Flexible Path Selection

In "Fig. 2", compare the MANET and NEMO communication models inside an MFS. In both scenarios, the mobile node (MN1) attached to MR4 communicates with the mobile node (MN2) attached to MR8. When the NEMO protocol is applied, the packets are routed toward the infrastructure to reach the home agents and return to the MFS. Since there are multiple mobile routers on the path between MN1 and MN2, multiple encapsulations occur. On the other hand, in the MANET scenario, mobile routers maintain the ad hoc links and manage local routing information. The path between MN1 and MN2 is directly established without relying on the fixed infrastructure.

One of the aims of MANEMO is flexible path selection depending on the MFS environment and communication conditions. An issue found within the MANET communication model is that the majority of the MANET routing protocols select the shortest path in all cases. This causes congestion at some links when many nodes generate traffic. For example, the MR7 link may become a possible bottleneck when the shortest path is taken.

In an MFS, infrastructure is available. Therefore, the mobile router transmits packets to the infrastructure even if the destination node is located nearby. Even though the path length may increase, the path over the Internet is often more reliable than the shortest ad hoc link. The additional overhead associated with transmitting packets to the infrastructure is a trade-off of several aspects such as latency, congestion, reliability, and cost of local routing management over wireless links. Each mobile router should be able to decide whether packets are routed to the infrastructure or to the destination directly over the ad hoc links. Other issues involving the use of fixed infrastructure by mobile routers are described in Section B

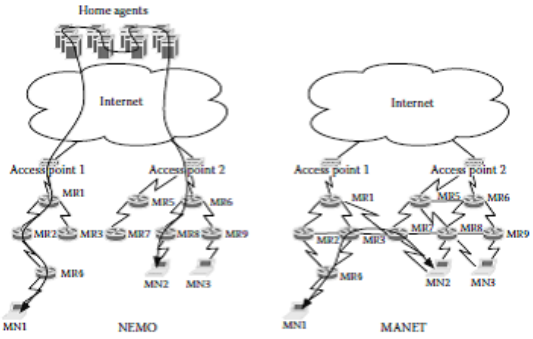


Figure 2: NEMO and MANET communication models

### B. Avoiding Redundant Tunnels and Paths

When multiple mobile routers are connected in a nested formation, redundant tunnels and UN optimized paths are often found. This is a well-known constraint of the NEMO basic support protocol. The NEMO basic support protocol does not provide any route optimization mechanism and mandates all traffic from and to a mobile router going through a home agent over a bidirectional tunnel. The route optimization has been investigated and summarized by Ng et al.

In "Fig. 2", the path from a mobile network node (MN1) to another (MN2) becomes MN1->MR4->MR2->MR1->HA1->HA2->HA4->HA8->HA6->MR6->MR8->MN2. Note that if MN1 and MN2 are visiting mobile nodes, two home agents are added to the path above. The path is clearly redundant compared to the MANET approach. In addition, whenever packets are routed over a mobile router, an additional IPv6 header is inserted in the packet for tunneling. Therefore, fragmentation may occur due to the availability of multiple tunnels between end nodes. Since the MFS is formed with resource-scarce wireless technology, larger packets hinder communication performance. MANEMO is expected to reduce the overhead of the bidirectional tunnels caused by the nested NEMO.

### C. Forming Loop-Free MFS

A network loop occurs when two mobile routers are connected to each other.

In "Fig. 2", MR2 can connect to the mobile network of MR4. The loop occurs between MR2 and MR4. Because the mobile network is seen as a regular IPv6 network, nodes connecting to the mobile network are unable to distinguish whether the attached network is mobile or not. The Internet reach ability of a mobile router is not always guaranteed due to the mobile router's movement. If the mobile router does not register the binding to its home agent, the mobile network is equivalent to a disconnected link. MANEMO provides useful information on access link conditions to nodes attached to the MFS. In

  

addition, MANEMO provides a mechanism to form the MFS loop-free.

### D. Supporting Movement Transparency

When a mobile router changes its point of attachment, it must hide the changes from any nodes located within its mobile network. Since nodes in the mobile network move together, sets of mobile routers can move at once in an MFS.

In "Fig. 2", MR2 moves its point of attachment from MR1 to MR3. The movement has minimum impact on MR4 and MN1 under the MR2. On the other hand, under most MANET and AUTOCONF schemes, the change of MR4's attachment affects the neighboring nodes (and possibly the entire network). Most routing protocols require route recalculation or route rediscovery (route maintenance) when topology changes take place. This should be avoided as it breaks the nature of the NEMO basic support protocol. MANEMO inherits from NEMO and supports movement transparency when a mobile router changes its attachment point.

### E. Supporting Diversity of Wireless Access

An MFS is formed with multiple wireless access technology such as WiMAX, Wi-Fi infrastructure mode, LTE, and even Wi-Fi ad hoc mode (802.11p). This is possible as each mobile router has at least two interfaces such as egress and ingress interfaces. Moreover, a mobile router (e.g., in a vehicle) might have more egress interfaces for the high capability of the network connectivity. On the other hand, in most MANET scenarios, a MANET router uses the same wireless access media (e.g., 802.11b ad hoc mode) in the same MANET because of the flooding capability. MANEMO should support the diversity of wireless access media.

### F. Supporting Home Agent-Independent Communication

Mobile IPv6 and the NEMO basic support protocol rely on an entity called a home agent. Without registering the binding to the home agent, mobile nodes and routers cannot send or receive packets from foreign links. However, Internet connectivity is not always available in mobile scenarios and is often intermittent. In an MFS, there are multiple mobile routers (i.e., wireless links) along the path toward the Internet. Specifically when two mobile routers in the same MFS communicate, packets are not necessarily routed to the infrastructure. If local routing is available in the MFS, packets can be routed directly to the destination without involving home agents. MANEMO should support local routing inside the MFS and decrease the dependency of home agents on Mobile IPv6 and NEMO basic support protocols.

### G. Supporting Local Routing

In MANET, each router can route the packet received at the MANET interface. A route can receive a packet from a MANET interface and can send the packet from the same MANET interface according to its routing table. But in NEMO, a mobile router can route only the tunneled packet to and from its mobile network. Without the bidirectional tunnel, the mobile router never routes the non tunneled packet. The packet sent from the mobile network is always routed to the mobile router's home agent by using IP encapsulation. Incoming packets must be always tunneled from the mobile router's home agent except for packets meant for the mobile node itself.

## IV. MANEMO SCENARIOS: VEHICULAR,DISASTER, AND PUBLIC SAFETY NETWORKS

Since MANEMO supports network connectivity, ad hoc communication (infra structure less), self-forming, movement transparency, and diversity of wireless access media, real deployment scenarios for mobile computing naturally can expect to receive benefit from MANEMO technology. Examples of such possible scenarios are mesh networks, sensor networks, vehicle networks, personal area networks, disaster networks, and ship networks.

### A. Vehicular Network

Once mobile routers are well deployed in vehicles, personal devices, and the like, it is expected that we will begin to see access networks that are on the move. The best access network for users might depend on more than layer 2 information and location knowledge. For instance, a passenger in a vehicle (e.g., bus or train) should connect to the access network provided by that vehicle while a stationary passenger located in the station should get access from a fixed resource. Some of the required information to make the proper decision should be delivered to users. MANEMO is a mechanism employed to discover and select the best access network for users. The MANEMO scenarios are very close to our daily life and related to human movement patterns.

The vehicle network for vehicle to vehicle (V2V) and vehicle to road (V2R) communications is another possible MANEMO scenario. While a mobile router will be deployed on a vehicle and provide network connectivity to nodes inside the vehicle, the vehicle needs to communicate locally to the vehicle driving in front or to road-side units. These local communications are not always served by the mobile router because of the cost of communications, the ad hoc nature of communications, and the existence of delay sensitive communications (e.g., safety applications). MANEMO can be a good solution candidate for future vehicular networks.

### B. Disaster and Public Safety Network

Disaster and public safety scenarios are another hot topic related to MANEMO. The MetroNet6 project was introduced as an example of a possible MANEMO scenario by Jim Bound (HP Fellow) in IETF. The MetroNet6 is developing dynamic, secure wireless networks formed with both wireless and wire line access media in an ad hoc manner for first responders to

  

disaster cases. Its aim is to connect police, firefighters, and hospitals to a command center (e.g., National Homeland Security Office) over the MetroNet6 and the Internet infrastructure in the event of a disaster. All personnel involved in the disaster recovery are equipped with wireless handheld devices for voice, video, medical and any data communication over the MetroNet6 infrastructure. The project began in the state of California (Sacramento). The network expected to be deployed under the MetroNet6 project is very close to the characteristics of a MANEMO. In Europe, there is a similar activity called U-2010 project developing a ubiquitous IP infrastructure for effective and flexible communication in disaster and public safety arenas. In Asia, after the Indian Ocean tsunami struck in 2004, several projects were started for disaster recovery networking. The Digital Ubiquitous Mobile Broadband OLSR (DUMBO) project aims at providing dynamic wireless ad hoc networks for disaster scenarios in Thailand.

A common feature of these projects is the quick recovery of communication infrastructure and flexible connectivity management by combining dynamic wireless networks and existing wire line infrastructure (e.g., Internet). For MANEMO, many mobile routers on emergency vehicles, military vehicles, and rescue crews are deployed in the disaster area and form an MFS to restore connectivity. The MFS might be disconnected initially due to the complete breakdown of the infrastructure, but it can be extended later to the Internet over wireless connectivity (satellite) from emergency vehicles. The MFS can be used for local recovery actions and also for remote recovery actions from remote command centers.

### C. Scenario Analysis

When MANEMO scenarios are analyzed, there are several features such as:

1. **Group mobility :** Nodes in an MFS move as a group. Nodes do not move randomly in MANEMO scenarios. Nodes often move within a set of groups. For instance, passenger nodes are moved together with a vehicle. Alternatively, MANET routing protocols address the random movement of nodes. Vehicles driving on a highway are sometimes moving together for a while.
2. **Less mobility :** The topology of an MFS does not change frequently in MANEMO scenarios. The majority of scenarios deal with vehicle networks. Once nodes board a vehicle, the topology inside the vehicle does not change until the nodes disembark from the vehicle. On the other hand, topology might be frequently changed in vehicle to vehicle networks depending on wireless Medias and the moving speed of vehicles. There are less topology changes when vehicles are in a traffic jam.
3. **Internet-oriented communication :** Communications tend to be established between nodes in an MFS and in an infrastructure. Local communication in the same MFS occurs rarely, as participants in an MFS do not have a strong relationship with each other in MANEMO scenarios. For example, in a train, all passenger communications are established with nodes in the infrastructure (e.g., Internet). Therefore, a solution should be designed to support global communications to and from an MFS.

## V. MANEMO ARCHITECTURE

This section outlines the MANEMO architecture including envisioned topology configuration and addressing assignments.

### A. The NEMO Basic Support Protocol

Before explaining the MANEMO architecture, we mention the architecture of the NEMO basic support protocol. A mobile network is defined in RFC 3753 as, "An entire network, moving as a unit, which dynamically changes its point of attachment to the Internet and thus its reach ability in the topology. The mobile network is composed of one or more IP-subnets and is connected to the global Internet via one or more Mobile Routers (MR). The internal configuration of the mobile network is assumed to be relatively stable with respect to the MR". A mobile network is seen as an IPv6 subnet by any nodes other than mobile routers.

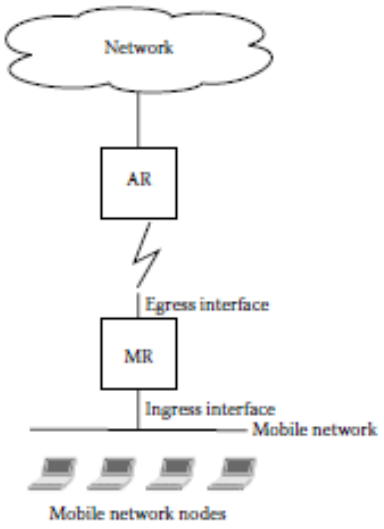


Figure 3: The mobile router's configuration

In "Fig. 3", According to RFC 3963 is the common interpretation of a mobile router. Each mobile router has an egress interface(s) to reach the home agent through the Internet and also an ingress interface attaching to the mobile network. A mobile network node is a node attached to the mobile network such as fixed or mobile routers and fixed or mobile hosts. A mobile router obtains its care-of address at the egress interface and establishes a bidirectional tunnel to the home agent. It routes all packets intercepted at the ingress interface to the bidirectional tunnel. A packet's source address must belong to the mobile network prefix. Only packets sent to and from a mobile network are routed to the tunnel by the mobile router. Some known remarks from this NEMO basic support are :

  

- Unless a mobile network node (host or router) is connected to a mobile network, NEMO guarantees session continuity to the node.
- Mobile network nodes are not aware of the mobile router's changing attachment point. The mobile network can be seen as just an IPv6 network.
- An access router at a visiting network is not aware of the existence of a mobile network behind the mobile router.

## B. MANEMO Topologies

The NEMO basic support protocol uses two different interfaces on a mobile router known as the egress interface and the ingress interface as explained. These interfaces are not necessarily physically available. If we interpret egress and ingress interfaces as conceptually defined interfaces, a mobile router can be operated with a single physical interface defining both the ingress and egress functions. In MANEMO, several topologies can be realized through the attachment of a combination of these two interfaces.

In "Fig. 4" shows all the possible topologies of MANEMO. When considering MANEMO, the following topology can be logically possible. The MFS is formed either by one of these topologies or a combination of the topologies listed below.

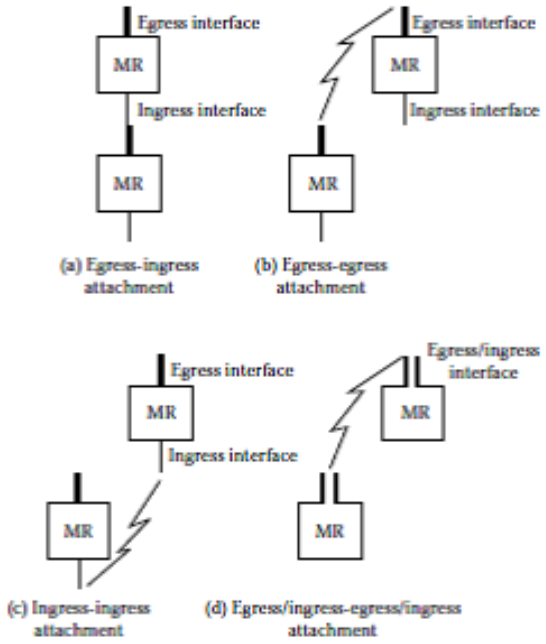


Figure 4: MANEMO topologies

1. **Egress and ingress (E-I) attachment (Figure 4a) :** The E-I attachment is the common configuration of the NEMO basic support. A mobile router connects to the other mobile routers' mobile network by its egress interface. A mobile router of a personal area network of a driver can connect to a mobile router of a vehicle by E-I attachment.
2. **Egress and egress (E-E) attachment (Figure 4b) :** The E-E attachment is found when a mobile router uses an ad hoc type of interface such as 802.11b ad hoc mode, 802.11s, or 802.11p as its egress interface. Mobile routers connect to each other by egress interfaces. This configuration is similar to MANET topology. In MANEMO, this scenario is also considered for inter vehicle networks (VANET).
3. **Ingress and ingress (I-I) attachment (Figure 4c) :** Although this configuration is logically possible, it is slightly unrealistic. When ingress interfaces of different mobile routers are connected, two different mobile networks are merged into a single mobile network. A mobile network node will obtain multiple IP addresses from different mobile routers. Whenever a mobile router leaves the MFS, addresses generated from the mobile network prefix of the departing mobile router become unreachable. This configuration may break the fundamental features of the NEMO basic support protocol due to the lack of movement transparency. This configuration is not considered in MANEMO.
4. **Egress/ingress and Egress/ingress (EI-EI) attachment (Figure 4d) :** EI-EI is a similar configuration to the E-E attachment. A mobile router is equipped only with a single wireless interface and uses it conceptually as both the egress and ingress interface. Under NEMO basic support, a mobile router is assumed to have two physically different interfaces. However, in this context, the ingress and egress interfaces are provided over the same physical interface. A mobile router exposes its mobile network prefix to the interface and also obtains a care-of address at the same interface.

## C. Addressing Architecture

The addressing architecture is an important factor in the design of a MANEMO solution. It brings several constraints to communication and routing. Each mobile router needs to obtain an address as a care-of address for the egress interface at visiting networks. This care-of address is used to exchange signaling and also to tunnel packets to the home agent. There are two different addressing assignment approaches today in IETF: the NEMO addressing approach and the AUTOCONF addressing approach. The main difference is where the address originates from.

In "Fig. 5", the arrows show how each mobile router and node obtains an address in MFS. In the NEMO addressing approach, the address is obtained from the upper router. If the upper router is a mobile router, the address is retrieved from the mobile network prefix of the mobile router. This is the basic concept of the NEMO basic support protocol. The node in the MFS is not aware of routers other than the upper router to which the node is attached. The movements of other routers are hidden by the upper mobile router. The address assigned to the node is not a topologically correct address, but it is defined at the home link of the upper mobile router. Therefore, all packets sent from the address are routed to the home agent by the upper mobile router. This is the origin of

  

the nested NEMO problem in MFS.

In the context of the MANET architecture, the egress interface of each mobile router can be treated as a MANET interface. The MANET architecture suggests assigning a unique address or prefix to the MANET interface. Although no solution has been defined for the MANET address assignment mechanism yet, the MANET addressing approach assumes that the address of each router in the MFS is derived from the exit router over multihops. To deliver addressing configuration information from the exit router, it is mandatory to maintain the local path between each router and the exit router. This is actually the natural behavior of MANET and its routing protocols. Unlike the NEMO addressing approach, whenever the MFS topology is altered due to the movement of one or more routers, this movement affects all nodes (or nodes behind the moving routers). Each node may update local routes by a MANET routing protocol. It is also required to update its address whenever the associating exit router is modified. The address is a topologically correct address that the exit router is serving. Packets are forwarded locally inside the MFS and routed to the destination by the exit router as required. There might not be a constraint that requires packets to travel all the way to the home network.

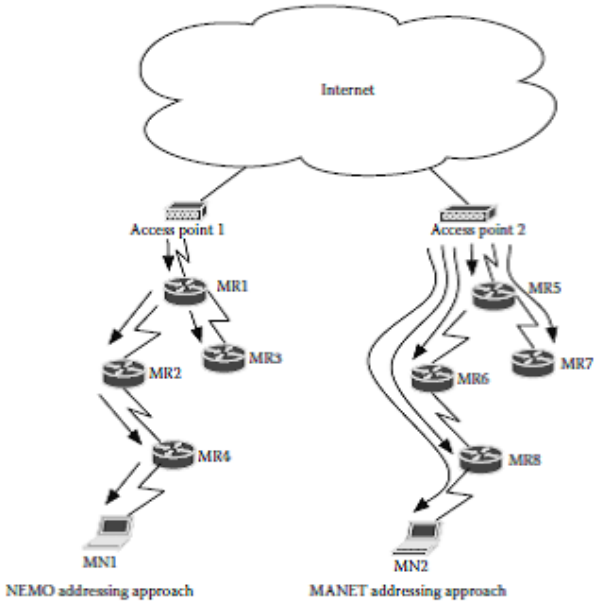


Figure 5: MANEMO topologies

However, there are several unclear and undefined areas to address toward achieving the MANEMO goals. Each mobile router obtains multiple, varying addresses on its egress interface such as one from the access router and one from its upper mobile router. Each mobile router runs IPv6 address auto configuration at the attached link (i.e., mobile network of the attached mobile router). As an example, MR8 obtains an address from the exit router (Access Point2) and another address from the upper mobile router, MR6. The mobile router selects the address assigned from the access router as a care-of address and registers it to the home agent. By doing so, tunnel overhead issues raised in the MANEMO problem statement are generally avoided. The packet is directly routed to and from the MFS via only the mobile router's home agent even if multiple mobile routers are located in the path of end nodes. Once the packet arrives at the MFS, it is routed to the target mobile router by MANET local routing.

An additional consideration is that the mobile router has its own mobile network prefixes and additional addresses on its ingress interface. Therefore, the mobile router must carefully check the source address of all packets to decide whether the packets should be routed to the bidirectional tunnel or not. If the packet is sent from the address of the mobile network, it is tunneled to the home agent. Otherwise, the packet is locally routed to the destination. If the destination is not in the same MFS, the packet is first delivered to the exit router and then routed to the destination in the infrastructure behind the exit router.

The loop-free topology formation is essential of MANET routing protocols. The multiple exits issue may be solved if the MANET routing protocol can be extended to carry additional information of exit routers along with the route information. Due to the local routing, if the destination and the source nodes are located in the same MFS, they can communicate without reaching the home agent.

## VI. SOLUTION CANDIDATES

Solutions are proposed for MANEMO in IETF. The existing solutions can be classified into a NEMO-centric and MANET-centric approach.

### A. MANEMO Solution Requirements

Before discussing and comparing the MANEMO solutions, we discuss the MANEMO solution requirements. Here are the lists of requirements proposed by Wakikawa et al :

1. The MANEMO protocol must enable the discovery of multi-hop topologies at layer 3 from mere reach ability and elaborate links for IPv6 usage, regardless of the wired or wireless media.
2. The MANEMO protocol must enable packets transmitted from mobile routers visiting the MFS to reach the Internet via an optimized path toward the nearest exit router and back.
3. MANEMO must enable IP connectivity within the nested NEMO whether the infrastructure is reachable or not.
4. The MANEMO protocol must enable packets transmitted from mobile routers visiting the MFS to reach the Internet with a topologically correct address.
5. The MANEMO protocol should aim at minimizing radio interference with itself as the control messages get propagated in the MFS.

  

6. The MANEMO protocol must enable inner movements within MFS to occur and ensure details of this movement are not propagated beyond the MFS.
7. An MFS may split to become two separate MFSs, in this case MANEMO will continue to maintain local connectivity within the separate MFSs and connectivity between the MFSs will be restored once a NEMO connection becomes available.
8. The MANEMO protocol should enable and optimize the trade-off between ensuring some reciprocity between MFS peers and maintaining a safe degree of CIA properties between the peer mobile routers.
9. The MANEMO protocol should enable the mobile routers to be deployed in restoring connectivity if parts of an MFS went isolated or extend the connectivity in the areas that are not covered.
10. The solution must not require modifications to any node other than nodes that participates in the MFS. It must support fixed nodes, mobile hosts, and mobile routers in the NEMO that form the MFS and ensure backward compatibility with other standards defined by the IETF.
11. The MANEMO protocol shall enable multicast communication for nodes within the MFS and on the Internet. Translation of MANEMO multicast signaling and multicast signaling on the Internet shall take place on the exit router.
12. The MANEMO protocol shall optimize the path to the Internet using cross-layer metrics.

The characteristics of "less mobility", "group mobility" and "Internet-oriented communication" are reasons for developing new solutions for MANEMO. Moreover, the following design decisions should be considered when developing a MANEMO solution.

In the MANET-centric approach, the assumption is one-to-all communication as the flooding mechanism is used for protocol operations. Flooding is used to disseminate packets to the entire MANET. Packets are delivered to all nodes in the MANET over multi hop. The flooding mechanism is not employed in the NEMO-centric approach. The proposed MANEMO protocols are operated one-to-one. A mobile router exchanges packets only with one-hop neighbors in the MFS. A packet is sometimes delivered beyond the one-hop neighbors, but it is always processed and routed by the intermediate nodes in the MFS. The one-to-all assumption brings with it various security issues. It is extremely difficult to establish secure relationships among all nodes in an MFS. Nodes in the MFS do not always share a common relationship in all MANEMO scenarios. MANET technology has not addressed security issues to this point in IETF. If security is not guaranteed in solutions, the MFS cannot be deployed and operated in real scenarios.

The MANEMO solution is to merge several features of several different protocols. As it is assumed MFSs will appear everywhere in the world, the MANEMO solution should be installed in all mobile devices similar to neighbor discovery protocol. The MANEMO solution should be one of the core networking protocols in a device. The solution should not introduce considerable overhead and modifications to the mobile device, since most mobile devices have limited computing and networking resources. Therefore, the trade-off between MANEMO solutions and MANEMO functions should be carefully considered. The MANET protocol may achieve most of the MANEMO goals; however, at the same time it might also introduce considerable overhead and modification to mobile devices.

As we discussed in Section.4, group mobility is a MANEMO-specific movement pattern. By using the NEMO basic support protocol, the impact of a mobile router changing attachment is hidden by that mobile router. Even if a mobile router changes its point of attachment, this change is perfectly hidden from nodes behind the mobile router. The topology behind the mobile router stays the same. On the other hand, in the MANET and AUTOCONF approach, the impact is propagated to all or some mobile routers that are located behind the mobile router which changes the attachment point. In the AUTOCONF addressing architecture, if a mobile router changes its attachment to a new access router, all nodes behind the mobile router should obtain a new address from the new access router.

## B. Solution Classification

Possible MANEMO solutions can be classified into two. The difference of these two approaches is which addressing architecture solution is selected (i.e. NEMO addressing architecture versus MANET addressing architecture).

1. **NEMO centric approach :** The nested NEMO is the initial root problem MANEMO seeks to address. Mobile routers attach to one another, and MANEMO should optimize the resulting topology for access to the infrastructure, provide a safe model for mobile routers to help one another, and offer some degree of inner routing. For this approach, tree discovery has been proposed to form a loop-free tree in MANEMO, and NINA provides some routing in that space. Reverse routing header (RRH) is a solution toward bypassing the number of home agents when mobile routers form a nested NEMO.
2. **Mobile ad hoc (MANET centric) :** NEMO mobile routers form a MANET in an MFS. If MANET approaches are taken, loop-free and local routing is somehow guaranteed. However, there are several optimized levels to be found by using different MANET mechanisms. The decision on which optimization level is ideal may depend on the MANEMO scenario under consideration.

## C. Tree Discovery

The tree discovery protocol is a distance vector protocol used to find the nearest exit toward the Internet and form a tree structure in the form of directed acyclic graphs. It is an extension to neighbor discovery protocol to carry information and metrics to form a loop-free tree structure in the MFS in an autonomous fashion. The tree information option is newly defined and carries the depth of the tree, the status of network connectivity, and so on by router advertisement down the tree. Although

  

each mobile router sends a router advertisement for its mobile network prefix, the tree information option is propagated down the tree. The value of the tree information option is updated by each intermediate mobile router in the tree structure. With the tree discovery protocol, the router can avoid the loop by carefully checking the tree-depth value advertised in the tree information option. A mobile router should not connect to another mobile router advertising a higher tree depth in order to avoid the loop.

In the tree information option, the status of connectivity to the infrastructure can be stored. By using such status, a mobile router can decide on the best tree with which to reach the infrastructure in an MFS. The tree depth is also one metric used to decide the tree head.

### D. Network in Node Advertisement

The network in node advertisement (NINA) protocol enables local routing between mobile routers in MFS. Local routing can prevent packets from going through multiple home agents between mobile routers in the same MFS. NINA exposes the mobile network prefixes up to the tree after tree discovery forms the loop-free tree structure. NINA defines a new option named network in node (NINO) option to carry the mobile network prefix in the neighbor advertisement message. By exchanging the NINO options by neighbor advertisement messages up to the tree, a mobile router learns the mobile network prefix of all other mobile routers down its tree. When two mobile routers in the same tree communicate, the upper mobile router of those two mobile routers can direct packets without going to the Internet. Since the cost of Internet connectivity in the mobile environment is expensive and unstable, local routing is beneficial in optimizing communication performance inside the MFS.

### E. Reverse Routing Header

The reverse routing header (RRH) is a source routing protocol used to avoid multiple tunnels and redundant routes in a nested NEMO. It introduces a new routing header called the reverse routing header and records the sequences of traversed mobile routers on the way out of an MFS. While the packet is forwarded along the tree formed by tree discovery, all the mobile router's care-of addresses are recorded in the reverse routing header of the packet. The reverse path is then recorded in each packet. Once the packet arrives at the MFS, it forwards the packet to a node in the MFS along the path recorded in the reverse routing header of the packet. It avoids multiple IP-in-IP tunnel encapsulations (40-byte header), while adding 16 bytes in the reverse routing header.

### F. MANET and AUTOCONF Solutions

MANET and AUTOCONF solutions are not specifically designed for MANEMO goals. However, there are several candidate solutions. The main goal of MANET and AUTOCONF solutions is to add local routing capability to mobile routers of the NEMO basic support protocol in an MFS.

For a simple solution, a mobile router only discovers the neighbor mobile router(s) and communicates only with it directly. Multihop capability is not available in this case. To add one-hop local routing capability, NANO provides a very simple solution to exchange the NEMO prefix between neighboring mobile routers. Similarly, NHDP is a candidate protocol for discovering two-hop neighbors. Although NHDP is designed to run with a MANET routing protocol, it is a protocol used to maintain two hop neighbors in the MANET. A mobile router manages routes for two-hop neighbor mobile routers and can optimize the path only for two-hop neighbors. No MANET routing protocols are required for one-hop and two-hop optimization of local routing.

If a MANET routing protocol such as the optimized link state routing protocol is run in the MFS, a mobile router can be made aware of the local route in the entire MFS and can form a loop-free topology in the MFS. MANEMO could still help in several fashions, for instance, providing scalability by splitting the larger network into a number of more manageable islands, interconnected by NEMO over the infrastructure.

## VII. CONCLUSION

This paper presents the MANEMO architecture and its goals. MANEMO has just begun the discussions in IETF and research community. As such the MANEMO concept is not well understood and has not been sufficiently addressed within IETF. However, several projects and individuals share a definite interest in the MANEMO concept and have begun work on solutions in IETF. It has been realized that MANEMO contains more issues than the nested NEMO problem. Several MANEMO solutions have been proposed and discussed, though a working group for MANET which has been formed within IETF. Following deployment of IP mobility technology, several mobile scenarios will surely move closer to what we have defined as MANEMO. The MANEMO will be the technology to mesh several features of different protocols.

## References

[1] Mobility Related Terminology. http://www.ietf.org/rfc/rfc3753.txt, 2004. RFC 3753, IETF.

[2] Network Mobility (NEMO) Basic Support Protocol. http://www.ietf.org/rfc/rfc3963.txt, 2005. RFC 3963, IETF.

[3] Mobility Support in IPv6. http://www.ietf.org/rfc/rfc3775.txt, 2004. RFC 3775, IETF.

[4] Problem Statement and Requirements for MANEMO. http://tools.ietf.org/id/draft-wakikawa-manemo-problem-statement-01.txt, 2007. Draft-wakikawa-manemo problem statement-01.txt, IETF, Internet Draft, (work in progress).

[5] MANEMO Topology and Addressing Architecture. http://tools.ietf.org/id/draft-wakikawa-

  

manemoarch-00.txt, 2007. Draft-wakikawa-manemoarch- 00.txt, IETF, Internet Draft, (work in progress).

[6] Nested Nemo Tree Discovery. http://tools.ietf.org/id/draft-thubert-tree-discovery-06.txt, 2007. Draftthubert-tree-discovery-06.txt, Internet Draft, (work in progress).

[7] Network In Node Advertisement. http://tools.ietf.org/id/draft-thubert-nina-00.txt, 2007. Draft-thubert-nina-00 (work in progress).

[8] IPv6 Reverse Routing Header and its application to Mobile Networks. http://tools.ietf.org/id/draftthubert-nemo-reverse-routing-header-06.txt, 2007. Draft-thubert-nemo-reverse-routing-header-06.txt, Internet Draft, IETF (work in progress).

[9] The NANO Draft (Scene Scenario for Mobile Routers and MNP in RA). http://tools.ietf.org/id/draft-petrescu-manemo-nano-00.txt, 2007. Draft-petrescu-manemo-nano-00 (work in progress).

[10] Network Mobility Route Optimisation Problem Statement. http://tools.ietf.org/id/draft-clausennemo-ro-problem-statement-00.txt, 2004. Draft-clausen-nemo-ro-problem-statement-00 (work in progress).

  