NEMO R. Baldessari
Internet-Draft NEC Europe
Intended status: Informational A. Festag
Expires: January 6, 2008 NEC Germany
M. Lenardi
Hitachi Europe
July 05, 2007

C2C-C Consortium Requirements for NEMO Route Optimization
draft-baldessari-c2ccc-nemo-req-01

Status of this Memo

Copyright Notice

Abstract

Vehicular ad hoc Networks (VANETs), self-organized networks based on short-range wireless technologies, aim at improving road safety and providing comfort and entertainment applications. The Car2Car Communication Consortium is defining a European standard for inter-vehicle communication that adopts VANETs principles. This document

specifies requirements for Route Optimization techniques for usage of Network Mobility (NEMO) in VANETs as identified by the Consortium.

Table of Contents

1. Introduction

In Vehicular ad hoc Networks (VANETs), cars are equipped with short-range wireless communication devices that operate at frequencies dedicated to safety and non-safety vehicular applications. When entering the proximity of each other, vehicles form a self-organized network by means of a specialized routing protocol that allows for packet exchange through broadcast and unicast communications. Further, fixed communication devices are installed along roadsides and can either distribute local warnings or offer connectivity with a network infrastructure. Due to its safety-oriented nature and extremely dynamic operational environment, this type of communication has lead research to consider specialized protocols and algorithms, especially concerning information dissemination, geographic distribution of packets and privacy/security issues.

The Car2Car Communication Consortium [10] is an industry consortium of car manufacturers and electronics suppliers that focuses on the definition of an European standard for vehicular communication protocols. The Consortium gathers results from research projects and aims at harmonizing their efforts. The first technical document [11], to be released in the following months, gives an overview of the system and protocol architecture, as well as of the applications on which the Consortium has agreed so far. In essence, this document defines a C2C-C protocol stack that offers specialized functionalities and interfaces to (primarily) safety-oriented applications and relies as a communication technology on a modified version of IEEE 802.11p [12]. This protocol stack is placed beside a traditional TCP/IP stack, based on IP version 6, which is used mainly for non-safety applications or potentially by any application that is not subject to strict delivery requirements, including Internet-based applications. The interaction between these stacks is currently discussed and briefly overviewed in this document.

As vehicles connecting to the Internet via dedicated access points (also termed Road Side Units, see Section 2 for terminology) change their attachment point while driving, the Consortium considers IP Mobility support as enhancing the system with session continuity and global reachability. When considering that passenger devices can be plugged into car communication equipment, therefore turning a vehicle into an entire moving network, Network Mobility (NEMO) principles have clear benefits in the discussed scenario (i.e. passenger devices shielded from mobility, centralized mobility management).

In NEMO Basic Support protocol [1] all data packets go through the IPv6-in-IPv6 tunnel established between the Mobile Router (MR) and the Home Agent (HA). As already pointed out in various documents ([7], [6] and [9]) this can have severe consequences on the

communication performances, as it causes data packets to follow a path that can be very far from optimal and requires a double IPv6 header for every packet exchanged with a Correspondent Node (CN) in the Internet. Compared with a communication that uses the ideal packet routing and the normal IPv6 header size, these factors results in an increased delay and a reduced throughput, plus indirect consequences like increased packet fragmentation and overall less efficient usage of resources. Even if, as described later, the C2C-C Consortium intends to adopt NEMO only for non-safety applications, a Route Optimization (RO) mechanism that alleviates or even eliminates this inefficiency is highly desirable. Moreover, the actual deployment of NEMO as default IP mobility support in C2C-C communication systems strongly depends on the availability of RO techniques.

The document is organized as follows: Section 2 defines terminology. Section 3 describes the technical approach of C2C-C Consortium that allows for usage of NEMO. Section 4 describes the deployment of NEMO in vehicular applications as intended by the C2C-C Consortium. Section 5 introduces the RO scenario and finally Section 6 lists the requirements for NEMO RO.

2. Terminology

The following terms used in this document are defined in the Mobile IPv6 protocol specification [2]:

- Home Agent (HA)

- Home Address (HoA)

The following terms used in this document are defined in the Mobile Network terminology document [8]:

- Network Mobility (NEMO)

- Mobile Network

- Mobile Router (MR)

- Mobile Network Prefix (MNP)

- Mobile Network Node (MNN)

The following terms used in this document are defined in the NEMO Route Optimization Space Analysis document [6]:

- o Correspondent Router (CR)

- o Correspondent Entity (CE)

The following new terms are used in this document:

- o On Board Unit (OBU): a device installed in vehicles, implementing the communication protocols and algorithm and equipped with at least 1) a short-range wireless network interface operating at dedicated frequencies and 2) a wireless or wired network interface where Application Units (AU) can be attached to. With respect to the NEMO terminology, the OBU is the physical machine acting as MR, 1) is used as egress interface and 2) as ingress.

- o Application Unit (AU): a portable or built-in device connected temporarily or permanently to the vehicle OBU. It is assumed that AUs support a standard TCP/IPv6 protocol stack, optionally enhanced with IP Mobility support. With respect to the NEMO terminology, an AU is a generic MNN.

- o Road Side Unit (RSU): a device installed along roadsides implementing the C2C-C communication protocols and algorithms. RSUs can either be isolated or connected to a network infrastructure. In the latter case, RSUs are attachment points either acting themselves as IPv6 access routers or as network bridges directly connected to an access router.

- o In-vehicle network: the wireless or wired network placed in a vehicle and composed by (potentially) several AUs and one OBU.

- o Vehicle-to-Vehicle (V2V) Communication Mode: a generic communication mode in which data packets are exchanged between two vehicles, either directly or by means of multi-hop routing, without involving any node in the infrastructure.

- o Vehicle-to-Infrastructure (V2I) Communication Mode: a generic communication mode in which data packets sent or received by a vehicle traverse a network infrastructure.

- o Vehicle-to-Infrastructure-to-Vehicle (V2I2V) Communication Mode: a generic communication mode in which data packets are exchanged between two vehicles, by means of multi-hop routing involving a RSU not connected to a network infrastructure.

3. C2C Communication Architecture

3.1. System Architecture

The current draft reference architecture of the C2C communication system is shown in Figure 1.

```
                        |       Internet        |
                        |                       |
                        +---+-----------------+-+
                            |                 |
                 Access  +--+-+            +--+-+  Access
                 Router  | AR |            | AR |  Router
                         +--+-+            +--+-+
                            |                 |
                      --+---+---            --+---+--
                        |                         |
         Road Side   +--+--+                   +--+--+   Public
           Unit      | RSU |                   | PHS |  Hot Spot
                     +---+-+                   +---+-+
                         |                         |
                        /\                        /\

                        \_                         \_
                          \_                         \_
                            \                          \

            Mandatory        \/
          Mod IEEE 802.11p    |       __               \/  Optional IEEE
            Interface     +---+--+      \__      \/     |   802.11a/b/g
                          | OBU1 |                |     |    Interface
                          +--+---+              +-+-----+---+
                   Vehicle1  |                  |   OBU2    |  On-Board
                        -+---+-+-               +--+--------+    Unit
                         |     |                   | Vehicle2
       Application    +--+-+ +-+--+           --+--+--
          Units       | AU | | AU |             |
                      +----+ +----+           +-+--+
                                              | AU |
                                              +----+
```

Figure 1: C2C-CC Reference Architecture

Vehicles are equipped with networks logically composed of an OBU and potentially multiple AUs. An AU is typically a dedicated device that executes a single or a set of applications and utilizes the OBU communication capabilities. An AU can be an integrated part of a vehicle and be permanently connected to an OBU. It can also be a

portable device such as laptop, PDA or game pad that can dynamically attach to (and detach from) an OBU. AU and OBU are usually connected with wired connection, but the connection can also be wireless, such as Bluetooth. The distinction between AU and OBU is logical, they can also reside in a single physical unit.

Vehicles' OBUs and stationary units along the road, termed road-side units (RSUs), form an ad hoc network. An OBU is at least equipped with a (short range) wireless communication device based on draft standard IEEE 802.11p [12] (adapted to European conditions and with specific C2C-C extensions) primarily dedicated for road safety, and potentially with other optional communication devices. OBUs directly communicate if wireless connectivity exist among them. In case of no direct connectivity, multi-hop communication is used, where data is forwarded from one OBU to another, until it reaches its destination. For example in Figure 1, RSU and OBU1 have direct connectivity, whereas OBU2 is out of RSU radio coverage but can communicate with it through multi-hop routing.

The primary role of an RSU is improvement of road safety. RSUs have two possible configuration modes: as isolated nodes, they execute applications and/or extend the coverage of the ad hoc network implementing routing functionalities. As attachment point connected to an infrastructure network, RSUs distribute information originated in the infrastructure and offer connectivity to the vehicles. As result, for example, the latter configuration allows AUs registered with an OBU to communicate with any host located in the Internet, when at least one RSU connected to a network infrastructure is available.

An OBU may also be equipped with alternative wireless technologies for both, safety and non-safety. For example, an OBU may also communicate with Internet nodes or servers via public wireless LAN hot spots (PHS) operated individually or by wireless Internet service providers. While RSUs for Internet access are typically set up with a controlled process by a C2C-C key stake holder, such as road administrators or other public authorities, public hot spots are usually set up in a less controlled environment. These two types of infrastructure access, RSU and PHS, also correspond to different applications types. Other communication technology, such as wide coverage/cellular networks (e.g. UMTS, GPRS) may also be optionally installed in OBUs, but their usage is currently considered out of scope of the C2C-CC Consortium.

The C2C-CC commonly refers to two main communication modes:

o in Vehicle-to-Vehicle (V2V) mode, data packets are exchanged directly between OBUs, either via multi-hop or not, without

involving any RSU;

o in Vehicle-to-Infrastructure mode (V2I), an OBU exchanges data packets through a RSU with an arbitrary node connected to the infrastructure (potentially another vehicle not attached to the same RSU).

3.2. Protocol Architecture

The protocol stack currently considered by C2C-CC for OBUs is depicted in Figure 2.

```
+--------------------+------------------+
|                    |                  |
|       C2C-CC       |     IP-based     |
|    Applications    |   Applications   |
|                    |                  |
+--------------------+------------------+
|                    |    TCP/UDP/...   |
|  C2C-CC Transport  +------------------+
|                    |                  |
+--------------------+-----+    IPv6    |
|                          |            |
|       C2C-CC Network     |            |
|                          |            |
+--------------------+-----+------------+
|      Modified      |  Standard WLAN   |
|    IEEE 802.11p    | IEEE 802.11a/b/g |
+--------------------+------------------+
```

Figure 2: OBU Protocol Stack

Protocol blocks are explained in the following list:

o Modified IEEE 802.11p: this block represents MAC and PHY layers of a wireless technology based upon current draft standard IEEE 802.11p [12] but modified for usage in Europe. In Europe, allocation of dedicated frequencies around 5.9 GHz for safety and non-safety applications is in progress. Expected communication range in line of sight is around 500m. This network interface is mandatory.

o IEEE 802.11a/b/g: this block represents MAC and PHY layers provided by one ore more IEEE 802.11a/b/g network interfaces. This network interface is optional but C2C-C Consortium encourages its installation.

- o C2C-CC Network: this block represents the network layer protocol currently defined by C2C-CC. The protocol provides secure ad hoc routing and forwarding, as well as addressing, error handling, packet sequencing, congestion control and efficient information dissemination. The specification of this protocol is currently under discussion. Only the C2C-CC Network protocol can access the Modified IEEE 802.11p network interface. The C2C-CC Network protocol can also access the IEEE 802.11a/b/g interface. The C2C-CC Network protocol offers an interface to the IPv6 protocol. This interface allows IPv6 headers and payload to be encapsulated into C2C-CC Network datagrams and sent over the Modified IEEE 802.11p or IEEE 802.11a/b/g network interface. The specification of this interface is currently under discussion. A primary goal of the C2C-CC Network layer is to provide geographic routing and addressing functionalities for cooperative safety applications. Through the mentioned interface to the IPv6 protocol, these functionalities are also available for IP-based applications.

- o C2C-CC Transport: this block represents the transport layer protocol currently defined by C2C-CC. This protocol provides a selected set of traditional transport layer functionalities (e.g. application data multiplexing/demultiplexing, connection establishment, reliability etc.). The specification of this protocol is currently under discussion.

- o C2C-CC Applications: this block represents the application layer protocol currently defined by C2C-CC and concerns Active Safety and Traffic Efficiency Applications.

3.3. IPv6 Deployment

As described in Section 3.2, the C2C-CC includes IPv6 as mandatory part of its specified protocol architecture. Currently, three methods are discussed for transmission of IPv6 headers and their payload:

- o On the Modified IEEE 802.11p interface via the C2C-CC Network layer: in this method, IPv6 headers are encapsulated into C2C-CC Network headers and sent using dedicated frequencies for inter-vehicle communications. As the C2C-CC Network layer transparently provides ad hoc routing, from the IPv6 layer perspective other nodes (OBUs and RSU) are attached to the same link. The real broadcast domain, where IPv6 multicast headers are distributed to, is chosen by the C2C-CC Network layer according to the packet type. In particular, C2C-CC Network layer provides efficient flooding and geographically scoped broadcast mechanisms. With respect to a currently adopted terminology, introduced in [13], the C2C-C Consortium approach for usage of NEMO on the Modified

IEEE 802.11p is fully MANET-Centric, in the sense that the sub-IPv6 protocol layer provides routing and forwarding in the ad hoc network. This results in the ad hoc nature of VANETs being hidden from IPv6 layer. A comparison of approaches for VANETs can be found in [14]. The deployability of this method strongly depends on the future availability of dedicated frequencies for non-safety purposes in inter-vehicle communications. If frequencies for this purpose will not be allocated, only the left part of the protocol stack of Figure 2 can access the Modified IEEE 802.11p interface.

- On the IEEE 802.11a/b/g interface via the C2C-CC Network layer: in this method, IPv6 headers are encapsulated into C2C-CC Network headers and sent using license-free ISM frequency bands (wireless LAN). Except the network interface, this method is equivalent to the previous one.

- On the IEEE 802.11a/b/g interface directly: in this method, IPv6 headers are sent directly to the wireless LAN interface as specified by [5].

The following informational list briefly summarizes currently discussed design concepts:

- vehicles use only IPv6 addresses with as host part an EUI-64 identifier derived from the MAC address. Privacy issues described in [4] are strongly alleviated through the use of temporary, changing MAC addresses, which are assigned in a set to every vehicle (as part of their assigned "pseudonyms");

- when a RSU connected to a network infrastructure is available, an OBU configures a globally routable Care-of Address using stateless address configuration;

- when infrastructure access is not available, OBUs use addresses with as prefix part a predefined IPv6 prefix (either reserved for C2C-C communications or a general purpose one);

- RSU can either act as IPv6 Access Routers or as network bridges connected to external IPv6 Access Routers. Different Access Routers are responsible for announcing different network prefixes with global validity. As a consequence, when roaming between different Access Routers, vehicles experience layer 3 handovers.

In all the methods for use of IPv6 in C2C-CC systems as described above, the IPv6 layer is meant to be enhanced with Mobility Support. As a vehicle includes a set of attached devices (AUs), Network Mobility seems the most appropriate solution, allowing for a centralized management of mobility to be executed in OBUs.

4. Intended NEMO Deployment

4.1. Scope of NEMO

In VANETs based on IEEE 802.11 family, a limited amount of bandwidth is shared among a potentially high number of vehicles. Additionally applications for safety purposes have strict requirements in terms of delay, information dissemination and aggregation and secure ad hoc routing. This conflicting conditions have led research activities to consider different approaches compared with traditional, packet-centric network engineering. In particular, only through a more information-centric approach it seems possible to achieve functionalities like geographic distribution, information dissemination according to relevance, information aggregation using cross-layer analysis, plausibility checks at different protocol layers.

Taking these aspects into consideration, the C2C-C Consortium is defining a protocol stack mainly dedicated for vehicular safety communications. Applications that are not subject to these particular requirements must use the right part of the protocol stack of Figure 2. This implies that the usage of NEMO in vehicular communications does not target safety-of-life applications but rather less restrictive, non-safety applications.

Another important aspect for deployability is related to costs. A primary goal of the C2C-C Consortium is to achieve a spread diffusion in terms of vehicles equipped with communication devices and protocols. This implies that vehicles of different brands and classes should be equipped by default with a basic communication system, whereas differentiation of products can be achieved by offering additional services. NEMO, like any other solution based on IP Mobility support, relies on a service provider that guarantees global reachability at the Home Network Prefix by maintaining an Home Agent. As it does not seem realistic that every car owner will also subscribe for such a service, a set of limited applications based on IPv6 should be available even without Mobility Support. Therefore, NEMO modularity and interoperability with non-NEMO equipped vehicles has to be guaranteed.

4.2. Example Use Cases

In this section, the main use cases are listed that have been identified by the C2C-CC for usage of NEMO in inter-vehicle communications: notification services, peer-to-peer applications and upload/download services.

4.2.1. Notification Services

A generic notification service delivers information to subscribers by means of the Internet. After subscribing the service with a provider, a user is notified when updates are available. Example services are weather, traffic or news reports, as well as commercial and technical information from the car producer or other companies.

As the network address of a vehicle changes while the vehicle moves among different points of attachment, without NEMO each application should register the new address in order to receive information at the correct location. Service providers would need to update continuously the subscription data and would be able to track the users. Adopting NEMO, which provides global reachability at a reasonably constant identifier (e.g. Mobile Network Prefix), efficiency and location privacy improve considerably.

4.2.2. Peer-to-peer Applications

A generic peer-to-peer application exchanges data directly between vehicles, without contacting any application server. Data traffic goes through a network infrastructure (V2I or V2I2V) or directly between cars when the infrastructure is not available (V2V). Example applications are vehicle-to-vehicle instant messaging (chat) and off-line messaging (peer-to-peer email), vehicle-to-vehicle voice over IP and file exchange.

In this set of use cases, the same applications should be able to run in V2V and V2I mode. As applications should not be aware of routing nor addressing issues, they should use the same identifier for sessions and users (e.g. cars/drivers/passengers) independently of the communications mode. Possible approaches are either to adopt resolution mechanisms or actually maintain the same network identifier in both V2V and V2I modes. This could be achieved for example generalizing the concept of Mobile Network Prefix (MNP) and allowing a Mobile Router (OBU) to use it for V2V communications in absence of attachment points. By means of enforcing limited lifetime for IPv6 prefixes and due to the isolation of VANET clusters from the infrastructure (in V2V), this use of MNP should not introduce routing inconsistencies.

4.2.3. Upload and Download Services

A generic upload/download service via the Internet consists in simple file exchange procedures with servers located in the Internet.

As in vehicular scenarios the connectivity to the infrastructure is highly intermittent, network address' changes cause applications to

re-establish sessions in order to resume the exchange, which implies considerable overhead. Session re-establishment can be avoided adopting NEMO.

5. NEMO Route Optimization Scenarios

In this section, operational characteristics of the intended NEMO deployment are described that are relevant for the design of Route Optimization techniques. In particular a restriction of the general solution space for RO and motivations for RO requirements described in Section 6 are provided.

In most NEMO deployment scenarios, MRs have permanent connectivity to the infrastructure and Route Optimization techniques are mainly intended as extensions of MIPv6 RO, where communication assumes to take place always through a point of attachment (infrastructure-based RO). In VANETs based on wireless LAN technologies, the connectivity of moving vehicles to the infrastructure is intermittent due to limited coverage of access points. Nevertheless, direct communication among vehicles should be supported even when infrastructure access is not available. Because this case is strictly a peculiarity of the considered scenario, a technique to allow direct communication (single- and multi-hop) by exposing the MNP associated to vehicles will be studied by the C2C-CC as part of the sub-IPv6 C2C-CC Network layer. Once such a mechanism is available, it MAY also be used as RO technique between MRs located in their vicinity (infrastructure-less RO). The sub-IPv6 layer is responsible for making sure that this mechanism is scalable, reasonably secure (i.e. compared with current Internet level of security) and protects users' privacy. More details about infrastructure-less RO are out of the scope of this document.

A C2C-CC OBU MUST be capable of both infrastructure-based and infrastructure-less NEMO RO. When both techniques are simultaneously possible (e.g. two MRs that are reachable both via the infrastructure and directly in the ad hoc domain) the OBU should apply appropriate policies to choose one. The definition of such policies is out of scope of this document. Furthermore, the scope of this document is restricted to the specification of requirements for infrastructure-based NEMO RO techniques.

With respect to the classification of NEMO Route Optimization scenarios described in [6], the non-nested NEMO RO case (Section 3.1) is considered as the most important for the C2C-CC deployment. In fact, MIPv6-enabled AUs (i.e. VMNs) and nested Network Mobility are not considered in the C2C-CC use cases.

The requirements defined in this document refer to RO between MR and CR (Correspondent Router). According to C2C-CC use cases, the CR can be:

- a NEMO MR. For example the MR running on another vehicle or another mobile device connected to the Internet;

- a RO-enabled router, i.e. a router static or mobile that does not act as NEMO MR but is capable of establishing RO sessions with NEMO MRs. For example the access router serving a CN in the infrastructure that offers services to vehicles, or the access router serving RSUs installed along the road;

- a RO-enabled router collapsed into the CN, i.e. performing internal routing. For example RSUs installed along the road.

As consequence of the fact that connectivity to the infrastructure strongly depends on vehicles' mobility, two opposite situations are here considered as RO scenarios: vehicles passing by points of attachment while driving and vehicles connecting to the infrastructure while stopped or parked.

In the first case, the connectivity to the infrastructure is available only for short time intervals. Vehicles' applications exchange data packets with nodes in the infrastructure in form of short bursts, containing for example traffic updates or information about local points of interests. In this situation, providing prompt and reliable communication is more important than achieving optimal routing or highest available throughput. In particular, the additional delay for RO establishment with every CRs can have a considerable negative impact. Furthermore, in some situations the path through MR-HA tunnel might be considered more reliable and trustworthy than a direct one to the CR. In particular, the tunnel allows the MR to hide its CoA from the CR which results in a location privacy protection. Therefore:

- vehicles should be able to decide whether or not to switch to RO according to various criteria (e.g. speed, density and geographic location of attachment points, trustworthiness of CR etc.);

- a lightweight RO scheme providing some degree of optimization (e.g. direct MR-CR routing but with the same packet overhead due to tunneling) and requiring short establishment times is more likely to be selected.

Another aspect of the vehicular dynamic scenario is that communication involving the infrastructure takes place mostly with nodes dedicated for vehicular communications, like control centers,

notification points, infotainment service providers. In all of these cases, the Correspondent Router is a newly deployed device. Consequently, RO techniques for this scenario are not strictly required to be compatible with CNs implementing legacy MIPv6 RO.

In the case of low mobile or static vehicles, the characteristics of the connectivity allow for classical internet-based applications, involving multiple nodes in the infrastructure. This scenario presents less peculiarities than the dynamic one when compared with other NEMO deployments (considering that the sub-IPv6 C2C-CC layer presents a flat topology to NEMO).

Other requirements for RO pointed out in Section 6 like multihoming, security and privacy, are fundamental and not related to the dynamics of the scenario.

6. NEMO Route Optimization Requirements

The C2C-C Consortium has identified the following requirements for NEMO RO techniques.

6.1. Req 1 - Separability

A RO technique, including its establishment procedure, MUST have the ability to be bypassed by applications that desire to use bidirectional tunnels through the HA.

As explained in Section 5, in some scenarios due to the intermittent connectivity, it might not be beneficial to activate RO. Therefore, applications or other management instances in the OBU should be able to trigger the switching to RO according to appropriate criteria.

This requirement is also specified in [9].

6.2. Req 2 - MNN IPsec

A RO technique SHOULD allow MNNs connected to the MR to use IPsec as if they were connected to a regular access router.

This requirement comes from the fact that no assumption can be made on pre-existing trust relationships between passenger devices and the OBU. Therefore, passenger devices (assumed to run IPv6 without Mobility Support) should be able to use full IPsec functionalities when connecting to the infrastructure via a MR.

6.3. Req 3 - RO Security

A RO technique MUST prevent malicious nodes to claim false MNP ownership. In order to achieve this, a RO technique MAY make use of security features provided by the sub-IPv6 C2C-CC Network layer (e.g. cryptographic protection), but it MUST NOT introduce new security leaks for the C2C-CC applications or render their security measures ineffective.

It is required that the security level of a RO scheme is comparable with today's Internet, which is the same goal of MIPv6 Return Routability procedure. In addition to that, as data security is mandatory for safety applications targeted by the C2C-C Consortium and implemented in the left part of the protocol stack depicted in Figure 2, security features will be already implemented in a C2C-CC compliant OBU. The presence of this features might facilitate the design of a lightweight, yet secure, RO technique.

C2C-CC security mechanisms are currently discussed and further details are out of scope of this document. As informational references, see [16], [17] and [18].

6.4. Req 4 - Privacy Protection

A RO technique MUST not require that the MNP is revealed to all nodes in the visited network. Instead, a RO technique MUST allow for revealing the MNP only to selected nodes in the visited network. Furthermore, a RO technique SHOULD allow that MNP and HoA are not exchanged as clear text.

Privacy of drivers and passengers is mandatory for safety applications targeted by the C2C-C Consortium. Mechanisms to implement privacy in the left part of the protocol stack depicted in Figure 2 are currently discussed (e.g. "revocable pseudonimity", where pre-assigned, quasi-random and changing pseudonyms are used as MAC and sub-IPv6 layer identifiers).

When using the right part of the stack depicted in Figure 2 to access the Internet using IPv6, users will be aware that the level of privacy protection is decreased. Nevertheless, clear text information that could allow for linking changed pseudonyms by sending constant identifiers should be minimized or even prohibited. In particular, encryption of Home Address and Mobile Network Prefix in NEMO signaling should be considered (e.g. specified as optional mechanism in [3]).

C2C-CC privacy protection mechanisms are currently discussed and further details are out of scope of this document. As informational

reference, see [15].

6.5. Req 5 - Multihoming

A RO technique MUST allow a MR to be simultaneously connected to multiple access networks, having multiple prefixes and Care-Of Addresses in a MONAMI6 context.

In other words, it is required that a RO technique can be used on multiple communication technologies. Assuming that mechanisms for registering and handling multiple CoAs are provided from the MONAMI6 work, NEMO RO should be usable for every available CoA.

This requirement is also specified in [9].

6.6. Req 6 - Coexistence with Sub-IPv6 RO

A RO technique MUST allow for coexistence in the same OBU with a RO technique offered by the sub-IPv6 C2C-CC Network layer. The OBU MUST be able to choose which technique to use when both are simultaneously available.

The here mentioned sub-IPv6 RO technique is supposed to inject routes into the IPv6 routing table as result of a sub-IPv6 signaling between cars, without involving the infrastructure. A NEMO RO technique should not be disturbed by the sub-IPv6 RO technique.

7. IANA Considerations

This document does not require any IANA action.

8. Security Considerations

This document does not specify any protocol therefore does not create any security threat. However, it specifies requirements for a protocol that include security and privacy issues in VANETs as currently discussed in the C2C-C Consortium.

9. Acknowledgments

The authors would like to thank the members of the work groups PHY/MAC/NET and APP of the C2C-C Consortium and in particular Tim Leinmueller, Bernd Bochow, Andras Kovacs and Matthias Roeckl.

10. References

10.1. Normative References

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

[2] Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.

[3] Arkko, J., Devarapalli, V., and F. Dupont, "Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents", RFC 3776, June 2004.

[4] Narten, T. and R. Draves, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", RFC 3041, January 2001.

[5] Crawford, M., "Transmission of IPv6 Packets over Ethernet Networks", RFC 2464, December 1998.

[6] Ng, C., Zhao, F., Watari, M., and P. Thubert, "Network Mobility Route Optimization Solution Space Analysis", draft-ietf-nemo-ro-space-analysis (work in progress), September 2006.

[7] Ng, C., "Network Mobility Route Optimization Problem Statement", draft-ietf-nemo-ro-problem-statement-03 (work in progress), September 2006.

10.2. Informative References

[8] Ernst, T. and H. Lach, "Network Mobility Support Terminology", draft-ietf-nemo-terminology-06 (work in progress), November 2006.

[9] Eddy, W., Ivancic, W., and T. Davis, "NEMO Route Optimization Requirements for Operational Use in Aeronautics and Space Exploration Mobile Networks", draft-eddy-nemo-aero-reqs-00 (work in progress), April 2007.

[10] "Car2Car Communication Consortium Official Website", http://www.car-2-car.org/ .

[11] "Car2Car Communication Consortium Manifesto", http://www.car-2-car.org/index.php?id=570 , May 2007.

[12] "Draft Amendment to Standard for Information Technology .

Telecommunications and information exchange between systems . Local and Metropolitan networks . Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Amendment 3: Wireless Access in Vehicular Environments (WAVE)", IEEE P802.11p/D1.0, February 2006.

[13] McCarthy, B., Edwards, C., Dunmore, M., and R. Aguiar, "The Integration of Ad-hoc (MANET) and Mobile Networking (NEMO): Principles to Support Rescue Team Communication", Proc. of International Conference on Mobile Computing and Ubiquitous Networking (ICMU 2006), October 2006.

[14] Baldessari, R., Festag, A., and J. Abeille, "NEMO meets VANET: A Deployability Analysis of Network Mobility in Vehicular Communication", Proc.of 7th International Conference on ITS Telecommunications (ITST2007), June 2007.

[15] Fonseca, E., Festag, A., Baldessari, R., and R. Aguiar, "Support of Anonymity in VANETs - Putting Pseudonymity into Practice", Proc.of IEEE Wireless Communication and Networking Conference (WCNC2007), March 2007.

[16] Raya, M. and J. Hubaux, "The Security of Vehicular Ad Hoc Networks", Proc.of Workshop on Security of Ad Hoc and Sensor Networks (SASN2005), November 2005.

[17] Aijaz, A., Bochow, B., Doetzer, F., Festag, A., Gerlach, M., Leinmueller, T., and R. Kroh, "Attacks on Inter Vehicle Communication Systems - an Analysis", Proc.of International Workshop on Intelligent Transportation (WIT2006), March 2006.

[18] Fonseca, E. and A. Festag, "A Survey of Existing Approaches for Secure Ad Hoc Routing and Their Applicability to VANETS", NEC Technical Report NLE-PR-2006-19, March 2006.

Authors' Addresses

Roberto Baldessari
NEC Europe Network Laboratories
Kurfuersten-anlage 36
Heidelberg 69115
Germany

Phone: +49 6221 4342167
Email: roberto.baldessari@netlab.nec.de

Andreas Festag
NEC Deutschland GmbH
Kurfuersten-anlage 36
Heidelberg 69115
Germany

Phone: +49 6221 4342147
Email: andreas.festag@netlab.nec.de

Massimiliano Lenardi
Hitachi Europe SAS Sophia Antipolis Laboratory
Immeuble Le Theleme
1503 Route des Dolines
Valbonne F-06560
France

Phone: +33 489 874168
Email: massimiliano.lenardi@hitachi-eu.com

Full Copyright Statement

Intellectual Property

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).