VARON: Vehicular Ad-hoc Route Optimisation for NEMO

Carlos J. Bernardos [a,*] Ignacio Soto [a] María Calderón [a]
Fernando Boavida [b] Arturo Azcorra [a]

[a] *Universidad Carlos III de Madrid*
Avda. Universidad 30, 28911 Leganés (Spain)

[b] *University of Coimbra*
Polo II, 3030-290 Coimbra (Portugal)

Abstract

In this paper we analyse the provision of enhanced communications between vehicles. It is expected that vehicles will have several communication devices, and that a specialised node will provide external connectivity to these devices, i.e. the devices in the vehicle form a Mobile Network. We propose the use of Network Mobility communication solutions for providing access from the vehicles to an infrastructured network (e.g., the Internet) or for communication with other vehicles. The main contribution of this paper consists in a route optimisation solution for mobile networks – based on the use of mixed ad-hoc and infrastructure communications – that enables inter-vehicle communications to be improved in terms of bandwidth and delay. The mechanism provides the same level of security than today's IPv4 Internet, by means of reusing Mobile IPv6 security concepts, and the use of public key cryptography and Cryptographically Generated Addresses. The proposed solution is characterised and evaluated through extensive simulation, showing that it provides an efficient optimisation in vehicular communications.

Key words: Inter-vehicular communications, Network Mobility, VANET, NEMO, Route Optimisation

* Corresponding author.
Email addresses: cjbc@it.uc3m.es (Carlos J. Bernardos), isoto@it.uc3m.es (Ignacio Soto), maria@it.uc3m.es (María Calderón), boavida@dei.uc.pt (Fernando Boavida), azcorra@it.uc3m.es (Arturo Azcorra).

[1] This work has been partly supported by the Spanish Government under the POSEIDON (TSI2006-12507-C03-01) and IMPROVISA (TSI2005-07384-C03) projects.
[2] The work described in this paper is also partially based on results of IST FP6 Integrated Project DAIDALOS II. DAIDALOS II receives research funding from the European Community's Sixth Framework Programme. Apart from this, the European Commission has no

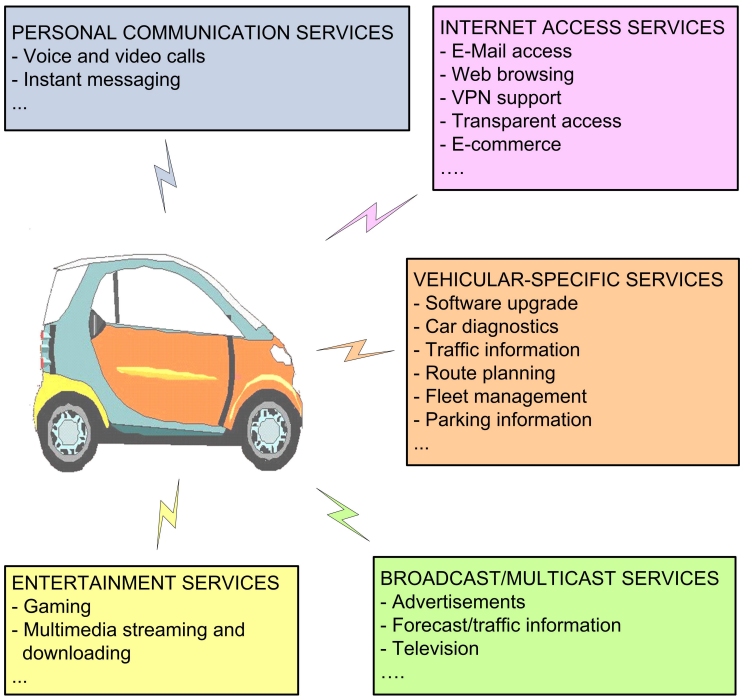


Figure 1. Some examples of applications and services in a vehicular scenario.

1 Introduction

Many people in modern societies spend a considerable amount of time in cars. Up to now, vehicular communications have been mainly restricted to cellular communication networks. Enabling broader communication facilities in cars is an important contribution to the global trend towards ubiquitous communications [1]. Vehicles should provide access to the Internet and also communication among themselves, supporting new services and applications.

Examples of services and applications (see Figure 1) that are of interest for automobile users are personal communication services, Internet access services, vehicular specific services such as traffic information or car diagnosis activities, entertainment services, and broadcast/multicast services. The provision of these services and applications in a vehicular scenario poses some challenges that require to be solved, mainly related to mobility management and security.

It is expected that several devices within a vehicle will likely benefit from having Internet connectivity (the so-called *car-to-Internet* scenario): internal sensors, on-board computers, infotainment back-seat boards, etc.; but also external devices, such as laptops or PDAs, carried by passengers. Therefore, our architectural as-

sumption is that networks will be deployed in cars, with specialised devices (Mobile Routers) providing nodes of these networks with the external communication access. A Mobile Router, as it will be described later, not only provides connectivity to the network deployed in the car, but also manages transparently the mobility of the whole network, without putting any additional requirements on the devices attached to the mobile network. Since it is expected that in forthcoming 4G networks multiple access technologies will be available, Mobile Routers will benefit from this heterogeneity by having more than one network interface (e.g., GPRS/UMTS, WLAN and Bluetooth, among others), allowing the Mobile Router to forward the traffic through the most appropriate interface. As an example, in vehicular environments, the use of additional WLAN interfaces may allow the creation of multi-hop ad-hoc networks by several vehicles, to optimise local (*car-to-car*) communications.

Besides the Internet access, there are several applications which involve a vehicle-to-vehicle communication. This kind of scenario may be supported by using Network Mobility solutions, so cars can communicate through the fixed infrastructure but, in this case, when the cars are close enough, a further optimisation is possible, namely to communicate directly using an ad-hoc network. In this way, better bandwidth than the one in the communication through the infrastructure can be achieved. Typically, this will be true even if we use a NEMO Route Optimisation solution for the communication through the fixed Internet. The reason is that, although the number of hops can be similar, the communication with the infrastructure will typically use a technology with lower bandwidth (for example, UMTS) than the ad-hoc network (for example, WLAN). Also, the ad-hoc route will probably result in lower costs.

This paper presents a Route Optimisation solution called *Vehicular Ad-hoc Route Optimisation for NEMO* (VARON). VARON allows local car-to-car communications to be optimised, by enabling – in a secure way – the use of a Vehicular Ad-hoc Network (VANET) for local communications among cars (instead of using the infrastructure). In VARON, communications security in the ad-hoc network is provided through use of the infrastructure, guarantying that the peer available through the ad-hoc network is the same that the one through the infrastructure. Besides, the robustness of VARON against ad-hoc routing attacks is build on the hop-by-hop authentication and message integrity of routing messages, and the use of Cryptographically Generated Addresses. However, this involves a performance cost, since cryptographic operations, such as signature generation/verification, consume time and energy. This cost could be of some concern, specially in energy and resource constrained devices. However, in the case of Mobile Routers deployed in cars, this is not a big issue, since vehicles have a powerful and rechargeable source of energy.

The remainder of this paper is organised as follows. A brief summary of the background and related work is provided in Section 2. Section 3 describes the security exploits that may appear in vehicular ad-hoc car-to-car optimisations. Our route op-

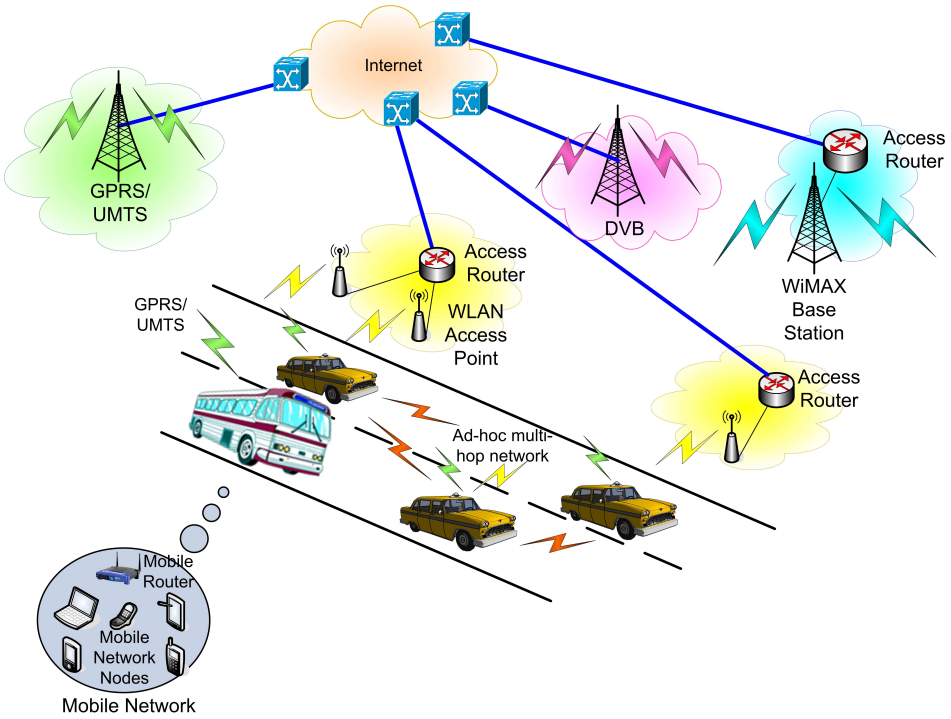


Figure 2. Vehicular communications scenario.

timisation mechanism for vehicular environments, VARON, is described in detail in Section 4. Section 5 evaluates VARON through simulations. Finally, Section 6 concludes the paper.

2 Background and Related work

This section summarises some of the concepts, terminology and related protocols that are used through the paper, and the related work and motivation for optimisation mechanisms in inter-vehicle communication scenarios.

2.1 Enabling Internet connectivity in automobiles: Network Mobility

Figure 2 shows an example of a vehicular scenario, that involves both communications between nodes inside a vehicle and the Internet, also called *car-to-Internet* communications (addressed in this section), and communications among vehicles, called *car-to-car* communications (addressed in Section 2.2).

There are several approaches that may be used to enable Internet access from automobiles. Initially, only cellular radio technologies were taken into account [2]. More recently, with the success of the IEEE 802.11 WLAN technology, it is being

investigated how to overcome the limitations of existing cellular radio networks (e.g., cost, low bandwidth, high delay, etc.), by making use of this technology and multi-hop *ad-hoc* protocols. As an example, the Drive-thru Internet project [3] proposed an architecture based on the deployment of several roadside IEEE 802.11 Access Points (APs) to enable Internet access from passing-by vehicles. One of the challenges posed by this architecture is that there could exist "holes" in the connectivity, that would prevent vehicles from communicating. In [3], a solution to mitigate this problem of intermittent connectivity is proposed, by means of a mechanism based on application gateways and proxies. Another drawback of this kind of solution is that it does not support transparent mobility among different technologies (e.g., a handover from WLAN to UMTS when no WLAN APs are available). The ability to switch among different access networks is critical for future 4G deployments.

Vehicular communication scenarios involve groups of devices moving together, so it seems more appropriate to use a network mobility approach [4], instead of host centric solutions, that would force each device within a car to manage its own connectivity to the Internet (including all the issues related to mobility).

The Network Mobility (NEMO) Basic Support protocol [5], proposed by the IETF [4], extends the basic end-host mobility solution, Mobile IPv6 [6], to provide network mobility support. In this solution, a mobile network (known also as *Network that Moves* – NEMO [5]) is defined as a network whose attachment point to the Internet varies with time. The router within the NEMO that connects to the Internet is called the Mobile Router (MR). It is assumed that the NEMO has a Home Network, connected to the Internet, where it resides when it is not moving. Since the NEMO is part of the Home Network, the Mobile Network Nodes (MNNs) have configured addresses belonging to one or more address blocks assigned to the Home Network: the Mobile Network Prefixes (MNPs). These addresses remain assigned to the NEMO even when it is away from home. Of course, these addresses only have topological meaning when the NEMO is at home. Thus, when the NEMO is away from home, packets addressed to the Mobile Network Nodes will still be routed to the Home Network. Additionally, when the NEMO is connected to a visited network, the MR acquires an address from the visited network, called the Care-of Address (CoA), where the routing architecture can deliver packets without any additional mechanism.

The goal of the network mobility support mechanisms [7] is to preserve established communications between the MNNs and their external Correspondent Nodes (CNs) despite movement. Packets of such communications will be addressed to the MNNs' addresses, which belong to the MNP, so an additional mechanism to for-

[3] `http://www.drive-thru-internet.org/`
[4] `http://www.ietf.org/`
[5] NEMO can mean NEtwork MObility or NEtwork that MOves according to the context.

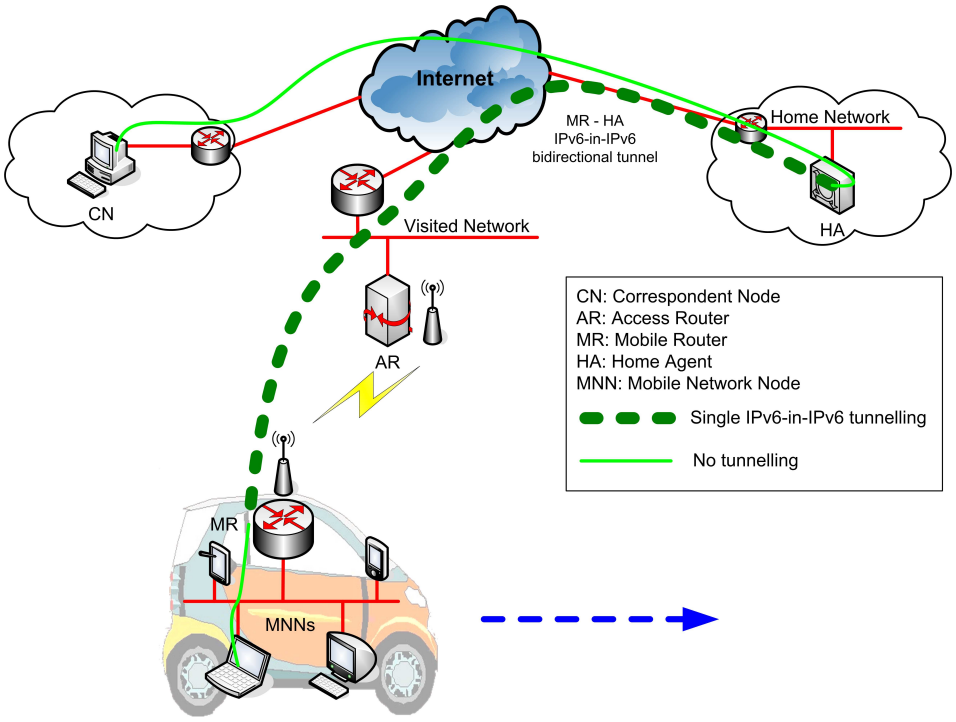


Figure 3. NEMO Basic Support protocol operation overview.

ward packets between the Home Network and the NEMO is defined. The basic solution for network mobility support [5] essentially creates a bidirectional tunnel between a special node located in the Home Network of the NEMO, called the Home Agent (HA), and the Care-of Address of the MR (see Figure 3).

The NEMO Basic Support protocol [5] has the following limitations:

- It forces suboptimal routing, i.e. packets are always forwarded through the HA, following a suboptimal path and therefore adding a delay in the packet delivery.
- It introduces non-negligible packet overhead, reducing the Path MTU (PMTU). Specifically, an additional IPv6 header (40 bytes) is added to every packet because of the MR-HA bidirectional tunnel.
- The HA becomes a bottleneck for the communication as well as a potential single point of failure. Even with a direct path available between an MNN and a CN, if the HA (or the path between the CN and the HA or between the HA and the MR) is not available, the communication is disrupted.

These problems are exacerbated when considering nested mobility (i.e. a mobile network gains connectivity through other mobile networks), since in this case the packets are forwarded through all the HAs of the upper level mobile networks involved.

Because of these limitations, it is highly desirable to provide what has been called *Route Optimisation (RO) support for NEMO* [8], to enable direct packet exchange between a CN (that is, any communication peer on the Internet) and a Mobile Net-

work Node (MNN), avoiding traversing the Home Network. There exist several NEMO RO proposals [9], [10] that eliminate or mitigate the aforementioned problems, although many of them require changes in the operation (i.e. upgrading the software) of CNs and/or MNNs and/or HAs. Furthermore, the additional load that may be required to perform new mobility functionalities to support a NEMO Route Optimisation mechanism, may be too high for certain devices within a car (e.g., sensors), because of their limited capabilities.

MIRON [11] is a proposal of a solution for Route Optimisation that does not require upgrades in CNs, MNNs, or HAs. MIRON has two modes of operation:

- The MR performs all the Route Optimisation tasks on behalf of those nodes that are not mobility capable – thus working as a Proxy MR [9].
- An additional mechanism, based on PANA [12] and DHCP [13], to support mobility-capable hosts (i.e. Mobile Nodes attached to a NEMO) and routers (i.e. nested Mobile Routers) that actually have mobility and Route Optimisation capabilities to manage their own Route Optimisation.

2.2 Optimising car-to-car communications

There exist several vehicular applications, such as multi-player gaming, instant messaging, traffic information or emergency services, that might involve communications among vehicles that are relatively close each other (i.e. car-to-car communications) and may even move together (e.g., military convoys). These applications are currently not well supported in vehicular scenarios.

Although automobiles can communicate with other vehicles through the infrastructure (the Internet) by means of the NEMO Basic Support protocol, they could benefit from better bandwidth, delay and, most probably, cheaper communication, by forming vehicular ad-hoc networks (VANETs) and making use of the resulting multi-hop network to directly communicate with each other. The challenge is to achieve this direct communication through the VANET with a security level equivalent to the one provided by today's IPv4 fixed Internet.

VARON enables to optimise car-to-car communications in a secure way by combining a Network Mobility approach – used to support car-to-Internet communications – with a vehicular ad-hoc approach – used when communication occurs between vehicles that are close enough to communicate through an ad-hoc network formed by the Mobile Routers deployed within those vehicles, and perhaps within other vehicles in their surroundings.

To the best of our knowledge, there is only one proposal, described in [14], that also proposes the combination of NEMO and ad-hoc approaches. The proposed mechanism in [14] assumes that each vehicle is a moving network and the performance of

inter-vehicular communications is improved by creating and using a VANET. The NEMO Basic Support protocol [5] is responsible for the provision of global Internet connectivity to the moving network, whereas an ad-hoc routing protocol is run among the Mobile Routers, creating an overlay VANET for inter mobile networks connectivity. This scheme enables direct communication between cars' devices that belong to the same overlay VANET (*direct route*), whereas the NEMO Basic Support protocol is used otherwise (*nemo route*). The problem with [14] is that it does not deal with the security aspects of the solution, and security is a critical issue for the feasibility of these kind of solutions.

Security is one of the main issues of this kind of solution in car-to-car environments, since the use of ad-hoc communications could enable malicious nodes to perform several types of attacks [15], such as stealing traffic or flooding a particular node. Next section describes the security challenges posed by the use of an ad-hoc solution for direct car-to-car communications, summarising and classifying the attacks that VARON aims at avoiding. As it will be explained in more detail in Section 4, VARON benefits from the simultaneous reachability of vehicles through the infrastructure and the ad-hoc network to secure the communications in the ad-hoc part.

3 Exploits against vehicular ad-hoc car-to-car optimisations

By using a Vehicular Ad-hoc Network to route packets of a local car-to-car communication, the performance of the communications in such a kind of scenario may be greatly improved – in terms of bandwidth and delay – when compared to data traversing an infrastructured network through a cellular radio network (e.g., UMTS). However, this kind of optimisation enables many different types of attacks. In this section, we briefly describe some relevant examples of attacks that would be possible if no additional mechanisms were used to secure this optimisation. This would help us introducing all the security problems that our proposal – VARON (described in Section 4) – avoids.

There are several types of attacks that may be performed against a vehicular ad-hoc car-to-car optimisation. Next, we describe the most relevant ones:

- *Prefix ownership attacks.* Devices within a vehicle form a mobile network, sharing a prefix (the Mobile Network Prefix), which is managed by the Mobile Router of the vehicle. It is necessary to provide Mobile Routers with a mechanism that enables them to mutually verify that a Mobile Router actually manages the Mobile Network Prefix it claims to (i.e. it is authorised to forward/receive packets addressed from/to that MNP). Otherwise, a malicious node would be allowed to spoof ("steal") a certain prefix and get all the traffic addressed to this prefix from other MRs connected to the ad-hoc network.

- *Ad-hoc routing attacks.* The creation and maintenance of the ad-hoc routes to locally exchange traffic between MRs connected to the VANET, is a critical issue from the security point of view. This task is performed by ad-hoc routing protocols, which still suffer from a lot of vulnerabilities, mainly due to the unmanaged and non-centralised nature of ad-hoc networks. Typical exploits against existing ad-hoc routing protocols may be classified into the following categories [16]:
  - *Modification attacks.* A malicious node can cause redirection of data traffic or Denial-of-Service (DoS) attacks by introducing changes in routing control packets or by forwarding routing messages with falsified values. As an example of this attack, a malicious node M could prevent a legitimate node A from receiving traffic from a node B by advertising a shorter route to B than the one that the true next hop towards A advertises.
  - *Impersonation attacks.* A malicious node can spoof the IP address of a legitimate node, and therefore *steal* its identity, and then perform this attack combined with a modification attack. The main problem of these attacks is that it is difficult to trace them back to the malicious node.
  - *Fabrication attacks.* A malicious node can create and send false routing messages. This kind of attack can be difficult to detect, since is not easy to verify that a particular routing message is invalid, specially when it claims that a neighbour cannot be reached.

Some ad-hoc secure protocols make impossible to perform some of these exploits (such as ARAN [16]). However, there is no mechanism that combines in a secure way a Network Mobility approach, to deal with the issue of vehicular global connectivity, and a Vehicular Ad-hoc Network, to optimise local car-to-car communications. By security, we mean a mechanism that is not vulnerable in the previously described ways.

4 Vehicular Ad-Hoc Route Optimisation for NEMO (VARON)

In this section we present a novel solution that provides Route Optimisation for NEMO in vehicular environments, where a Vehicular Ad-hoc Network (VANET) may be securely created and used to optimise local communications among vehicles.

It is assumed that the Mobile Router (MR) deployed in each vehicle will have at least three network interfaces: one *ingress* interface to communicate with the nodes inside the vehicle that belong to the NEMO (e.g., WLAN, Bluetooth), one or more *egress* interfaces to connect to the Internet (e.g., UMTS, WiMAX, even WLAN in some cases), and an additional ad-hoc interface (e.g., WLAN) to communicate with neighbouring cars and set-up multi-hop networks (see Figure 2). Compared with a normal Mobile Router (without any ad-hoc optimisation), only one (ad-hoc) additional interface is required. It is important to notice that Mobile Routers deployed

in vehicles will not be much concerned about energy or processing constraints, as opposed to personal mobile devices or other ad-hoc scenarios (such as sensor networks).

It is also assumed that vehicle's devices will be always able to communicate with other vehicle's devices through the Internet, by using the NEMO Basic Support protocol. On the other hand, there may exist the possibility of enabling these devices to directly communicate if a multi-hop vehicular ad-hoc network could be set-up by the involved vehicles and other neighbouring cars. VARON aims at making possible to benefit from this optimisation opportunity in a secure way.

In our proposal, VARON, the MR is the node in charge of performing the optimisation of the communications. The steps for carrying out this procedure are the following:

(1) *Discovery of reachable MNPs.* The MR needs to find out which other MRs are available within the VANET, that is, which Mobile Network Prefixes are reachable through its ad-hoc interface.
(2) *Creation of a secure ad-hoc route* between the MRs of the mobile networks that want to optimise the route they are using to exchange traffic. The ad-hoc routing protocol used to create this route should provide certain security guarantees making impossible to perform any of the exploits described in Section 3. The mechanism used by VARON to set-up and maintain a secure ad-hoc route is based on ARAN (Authenticated Routing for Ad-Hoc Networks) [16], modified and extended to fulfil the requirements of our Network Mobility based vehicular scenario.

Next, we describe in detail these two steps.

4.1 Discovery of reachable MNPs

Every MR announces its Mobile Network Prefix (MNP) by periodically broadcasting – through the ad-hoc interface – a message, called *Home Address Advertisement* (HoAA), that contains its Home Address and an associated lifetime, to allow this information to expire. These messages are announced through the ad-hoc interface, by using a hop-limited flooding, so every MR becomes aware of the MNPs that can be reached through the VANET.

The MR's HoA is chosen to belong to the NEMO's Mobile Network Prefix. The length of the MNP is fixed to 64 bits (/64) due to security reasons that will be explained later. Hence, the MNP can be inferred directly from the HoA (it is the network part of it). With the MRs' announcements, every MR is aware of all the MR's HoAs (and associated Mobile Network Prefixes) that are available within the ad-hoc network.

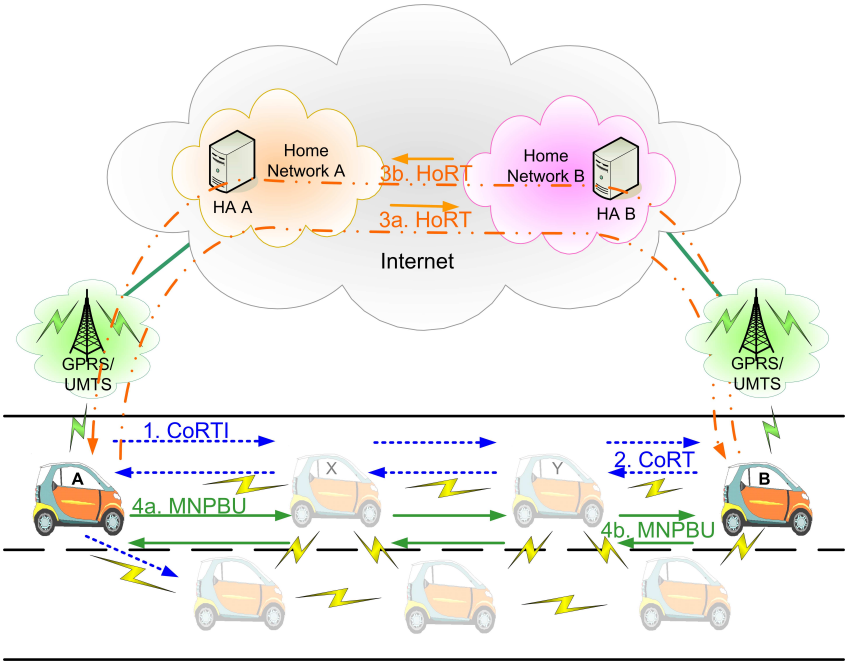


Figure 4. Care-of Route discovery and validation.

4.2 Creation of a secure ad-hoc route

4.2.1 Building the ad-hoc route

In case a Mobile Router detects that there is an ongoing communication between a node attached to it and a node attached to another MR that is available through the VANET and this communication is decided to be optimised (how this decision is taken is out of the scope of this paper), the MR needs to build a multi-hop route to send packets directly through the ad-hoc network.

An example (Figure 4) is used to illustrate in more detail the proposed mechanism. A device (e.g., a back-seat embedded video game system) in car A is communicating with another device in car B [6]. This communication is initially being forwarded through the Internet, following the suboptimal path determined by the NEMO Basic Support protocol, thus traversing Home Networks A and B before being delivered to the destination. We call this route *Home Route*. By listening to the announcements received in the ad-hoc interface, MR A becomes aware that the destination of such communication may be also reachable through a VANET formed by neighbouring VARON enabled vehicles. Then, MR A may decide to start using the vehicular ad-hoc network to route this traffic, instead of sending it through the Internet.

[6] Another example could be a car A from an emergency service convoy communicating with another emergency car B.

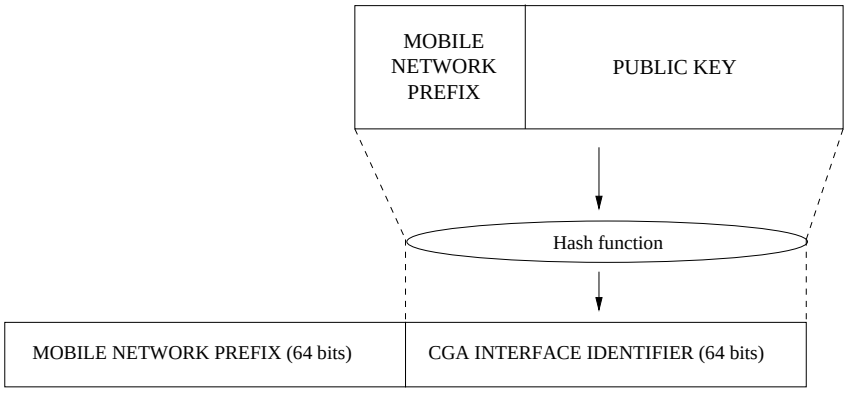


Figure 5. Simplified overview of CGA creation and structure.

The first step in this optimisation process is that MR A must learn and set-up a bidirectional route through the vehicular ad-hoc network to MR B (the MR claiming to manage MNP B). We call this route *Care-of Route*. For doing this, MR A (the *originator MR*) sends – through its ad-hoc interface – a *Care-of Route Test Init* (CoRTI) message (Table 1 summarises our notation) to its one-hop neighbours:

$$A \rightarrow \text{one-hop neighbours} :$$
$$[\mathbf{CoRTI}, HoA_B, N_A, HoA_A, K_{A+}]_{K_{A-}}$$

This message includes, besides the identifier of the message (CoRTI), the final destination MR's HoA (HoA_B), a nonce N_A (to uniquely identify a CoRTI message coming from a source; every time an MR initiates a route discovery, it increases the nonce), the IP address of MR A (HoA_A) and its public key (K_{A+}), all signed with the MR A's private key (K_{A-}). When an MR receives through its ad-hoc interface a CoRTI message, it sets up a reverse route back to HoA_A (MR A's HoA), by recording the MR from which it received the message (so it knows how to send a reply in case it receives a message that has to be sent back to HoA_A). In order to authenticate the message, a mechanism that securely binds the IP address of MR A (HoA_A) with K_{A+} is needed. One possibility is to use certificates issued by a third trusted party, as proposed in ARAN [16], but this solution seems unfeasible for vehicular environments. Instead, this secure binding is obtained by using a special type of addresses: Cryptographically Generated Addresses (CGAs) [17].

Cryptographically Generated Addresses (CGA) are basically IPv6 addresses for which the interface identifier is generated by computing a cryptographic one-way hash function from a public key and the IPv6 prefix [7]. The binding between the

[7] There are additional parameters that are also used to build a CGA, in order to enhance privacy, recover from address collision and make brute-force attacks unfeasible. We intentionally skip these details. The interested reader may refer to [17] for the complete procedure of CGA generation.

K_{A+}	Public Key (and CGA related information) of MR A
K_{A-}	Private Key of MR A
$[d]_{K_{A-}}$	Data d digitally signed by MR A
N_A	Nonce issued by MR A
HoA_A	Home Address of MR A
CoRTI	Care-of Route Test Init message type
CoRT	Care-of Route Test message type
CoRE	Care-of Route Error message type

Table 1
Table of variables and notation.

public key and the address can be verified by re-computing the hash function and comparing the result with the interface identifier (see Figure 5). In this way, if the HoA used by MRs is a CGA, a secure binding between the MR's HoA and the MR's public key is provided, without requiring any Public Key Infrastructure (PKI) to be available. Notice that by itself, CGAs do not provide any guarantee of prefix ownership, since any node can create a CGA from any particular Mobile Network Prefix by using its own public-private key pair. But a node cannot spoof the CGA that another node is legitimately using, because it does not have the private key associated with the public key of that IP address.

A receiving MR (e.g., MR X in Figure 4) uses MR A's public key (included in the message) to validate the signature, then appends its own public key (K_{X+}) to the message, and signs it using its private key (K_{X-}). The signature prevents spoofing or message modification attacks, that may alter the route or form loops. Then, it forwards the CoRTI message:

$$X \rightarrow \text{one-hop neighbours} :$$
$$\Big[[\mathbf{CoRTI}, HoA_B, N_A, HoA_A, K_{A+}]_{K_{A-}}, K_{X+}\Big]_{K_{X-}}$$

Upon receiving this CoRTI message from neighbour MR X, MR Y verifies the signatures from the originator MR A and the neighbour MR X, stores the received nonce to avoid reply attacks and adds a route to HoA_A through HoA_X (MR X). Then, the signature and public key of the neighbour MR X are removed, and MR Y appends its own public key, signs the message, and forwards it:

$$Y \rightarrow \text{one-hop neighbours} :$$
$$\Big[[\mathbf{CoRTI}, HoA_B, N_A, HoA_A, K_{A+}]_{K_{A-}}, K_{Y+}\Big]_{K_{Y-}}$$

This last step is repeated by any intermediate node along the path until the CoRTI message reaches the destination (the *target MR*, MR B) or the allowed hop limit expires. Notice that MR B, after receiving the CoRTI message, has the guarantee that only the node that has the private key associated with HoA_A (K_{A-}) could have sent the CoRTI message.

Once MR B receives the CoRTI message, it generates a reply message (including the received nonce N_A), called *Care-of Route Test* (CoRT), and unicasts it back following the previously learnt reverse path to the originator (MR A):

$$B \rightarrow Y :$$
$$[\mathbf{CoRT}, HoA_A, N_A, HoA_B, K_{B+}]_{K_{B-}}$$

Each node in the reverse path performs a procedure similar to the one performed forwarding the CoRTI: the first MR in the reverse path that forwards the message (i.e. MR Y) verifies the signature and, if correct, adds its public key K_{Y+}, signs the message and sends it to the next MR in the path:

$$Y \rightarrow X :$$
$$\left[[\mathbf{CoRT}, HoA_A, N_A, HoA_B, K_{B+}]_{K_{B-}}, K_{Y+}\right]_{K_{Y-}}$$

MR X also sets up a reverse route back to MR B's HoA by recording the MR from which it received the message.

The remaining MRs in the reverse multi-hop route, when receiving the CoRT message, verify the signature of the previous MR, remove it and the associated public key, add their public key, sign the message, forward it to the next MR, and set-up the reverse route. In the example, when MR X receives the message from MR Y, it sends the following to MR A:

$$X \rightarrow A :$$
$$\left[[\mathbf{CoRT}, HoA_A, N_A, HoA_B, K_{B+}]_{K_{B-}}, K_{X+}\right]_{K_{X-}}$$

When the originator MR (MR A in the example) receives the CoRT message, it verifies the signature and nonce returned by the destination MR (MR B). Once this procedure is completed, MR B has successfully established a route with MR A within the multi-hop vehicular ad-hoc network. This route is basically a temporal path (Care-of Route) to reach MR B's HoA, additional to the default route that MR A may always use to send packets towards MR B (through the Internet, using the Home Route), and vice-versa.

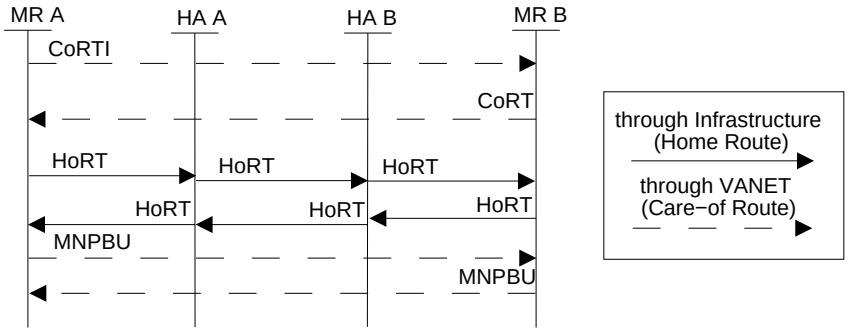


Figure 6. Care-of Route authentication signalling.

4.2.2 Authenticating the Care-of Route

The Care-of Route cannot be used to forward packets between NEMO A and NEMO B yet, since it has not been proved either that MR A manages MNP A, or that MR B manages MNP B. Only the validity of a route to a node (B and A) with an address (HoA_B and HoA_A) for which the node has the respective private key has been proved to MR A and MR B. It has not been verified that MR A and MR B are actually the routers authorised to manage MNP A and MNP B, respectively. Without further verification, nothing could prevent an MR from stealing a mobile network's traffic. For example, a malicious node could be able to claim the ownership of a given IP address (an address belonging to MNP A) and steal packets addressed to that prefix (MNP A). This issue is similar to that of Route Optimisation in Mobile IPv6, where a mechanism is required to enable the Mobile Node to prove that it *owns* both the Care-of Address and the Home Address.

The Return Routability procedure defined for Mobile IPv6 is based on two messages sent by the CN, one sent to the Mobile Node's Home Address and the other to Mobile Node's Care-of Address. Based on the content of the received messages, the Mobile Node sends a message to the Correspondent Node [6], [15]. By properly authenticating the message, this procedure is enough to prove that the Mobile Node has received both messages and therefore it has been assigned (that is, *owns*) both the Home Address and the Care-of Address at that time.

In VARON, we borrow from the Return Routability (RR) procedure some of the underlying security concepts. With the RR, the Correspondent Node is provided with a mechanism to verify that a Mobile Node is able to send and receive packets from two different addresses. In VARON, what is needed is to provide a pair of end-point MRs (which are communicating with each other through the Home Route) with a mechanism to verify that the multi-hop route within the VANET connects each of them with the same network (the respective MNP) that each MR can reach through the infrastructure when communicating with any address within the MNP of the other MR. In this way, the two end-point MRs may choose to use that Care-of Route instead of the Home Route.

The essence of the Care-of Route authentication procedure in VARON is that the

two end-point MRs involved in a particular Route Optimisation procedure request each other to verify that the VANET Care-of Route may be used to send traffic between the two NEMOs. This is done (see Figure 6) as follows:

- Each Mobile Router generates a key, K_{mr}, which can be used with any other MR. In addition, the MR generates nonces at regular intervals. These nonces [8] and K_{mr} will be used to generate a security association between the two end-points MRs.
- Each MR creates two tokens and sends each of them through one of the possible routes (Care-of and Home routes). Tokens are generated from K_{mr} and a particular nonce.
- The first part of the Care-of Route authentication procedure is done at the same time – and using the same messages – as the Care-of Route setup (described in section 4.2.1). The first token, called *Care-of keygen token*, is sent piggybacked in the CoRTI message, plus a *Care-of cookie*, and the index of the nonce used to generate the token. The correspondent MR replies in the CoRT message, including its own Care-of keygen token, its nonce index and copying the cookie received in the CoRTI message.
- The second token, called *Home keygen token*, is sent, plus a *Home cookie* and a nonce index, in a separate message, called *Home Route Test* (HoRT), through the MR-HA tunnel (protected by IPsec ESP in tunnel mode) configured by the NEMO Basic Support protocol, using the routing infrastructure. In order to verify that the correspondent MR is actually managing the IPv6 network prefix it claims to, that is, the Mobile Network Prefix assigned to the NEMO, the HoRT message is sent to a random address within the MNP. The MR that manages the prefix has to intercept [9] that message therefore showing that it actually manages the MNP [10] . The Mobile Network Prefix length used by VARON MRs is fixed to 64 bits (/64), in order to avoid a malicious node to "steal" a prefix. Otherwise, for instance, if an MR was assigned a /64 prefix, then with probability $1/2$ it could try to spoof a /63 prefix (and steal its *"neighbours"* packets). By fixing the MNP length, this attack is no longer feasible.

  As in the case of the Care-of Route test, the correspondent MR replies this message with another HoRT message, including its own Home keygen token and nonce index, and copying the received cookie.
- Each MR uses the received Home and Care-of keygen tokens to create a key, K_{bm} that can be used to authenticate a *Mobile Network Prefix Binding Update*

[8] Note that these nonces are different from the ones used during the ad-hoc route discovery and setup procedure.

[9] It is not required the MR to continuously examine every received packet in order to intercept HoRT messages. The MR may start inspecting packets after sending (or receiving) a CoRT message.

[10] This test does not guarantee that a node manages a certain prefix, but that this node is at least in the path toward that prefix. This provides the solution with a similar security level that today's IPv4 Internet has.

(MNPBU) message [11] – sent along the Care-of Route –, that enables the other MR to check that the Mobile Network (MNP) reachable through the VANET (Care-of Route) is the one reachable through the infrastructure. This verification can be done because each MR has the information required to produce the key when the MNPBU is received, and therefore authenticate the message.

At this point VARON signalling has finished. MR A has found out that MR B – which owns HoA_B and its associated private key and that is reachable through the VANET – is also capable of receiving and sending packets sent to any address from the Mobile Network Prefix (MNP) B through the infrastructure. This only happens if the HA responsible of routing packets addressed to this MNP (that is, HA B) is forwarding to MR B those packets addressed to MNP B. HA B only would be doing that if proper authentication has taken place and MR B is authorised to manage MNP B. The same guarantee also holds for MR B regarding MNP A and MR A.

The Care-of Route authentication mechanism performed in VARON, as the Return Routability procedure defined in Mobile IPv6, implicitly assumes that the fixed routing infrastructure is secure and trusted. As long as this is true, the mechanism defined is appropriate to secure the Mobile Network Prefix Binding Update, since it does not introduce any new vulnerabilities that were not possible in today's IPv4 Internet.

Once the process has been completed, the end-point MRs (MR A and MR B) may exchange traffic using the set-up Care-of Route within the VANET.

4.2.3 Optimised routing using the VANET

Once the Care-of Route authentication procedure has finished, all MRs involved in the creation of the ad-hoc route can forward packets to the HoAs of the end-point MRs (see an example in Figure 7). However, only the end-point MRs have verified the association of the corresponding MR' HoA and the respective MNP. Intermediate MRs (i.e. MR X and MR Y in the example) have only learnt host routes towards the Home Addresses of the two end-point MRs (i.e. HoA_A and HoA_B). In order to route data traffic between cars' nodes with addresses belonging to MNP A and MNP B, each end-point has to tunnel the packets towards the other MR's HoA, through the VANET route. In this way, intermediate MRs in the ad-hoc route just forward the packets based on the host routes (with the end-point MRs' HoAs as destination) added to their routing tables during the ad-hoc Care-of Route

[11] The generation of this key (K_{bm}) and the keygen tokens, and the authentication of the message follow the same mechanisms that the Return Routability procedure [6], [15] and the proposal to extend it to support network prefixes [18]. We explicitly avoid these details to make the paper more readable (the interested reader may refer to [6], [15] for additional information).

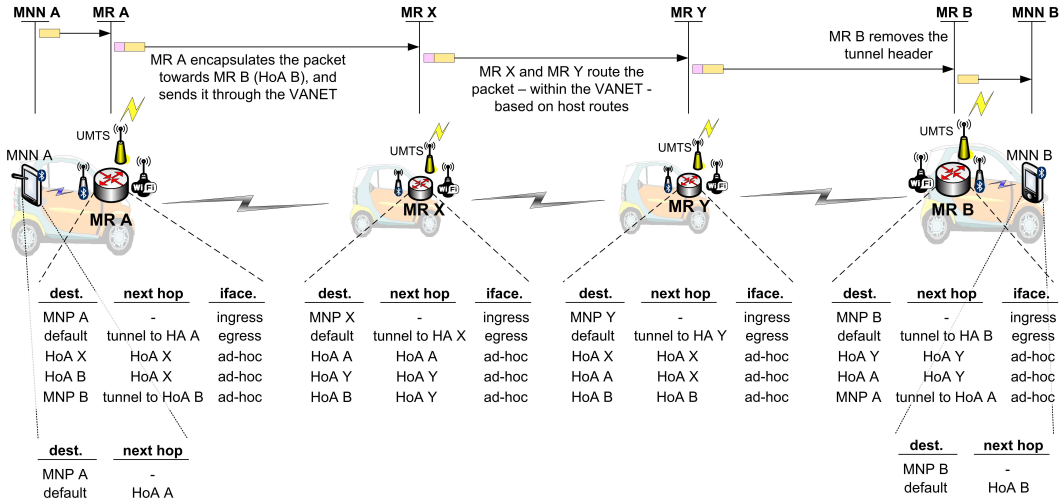


Figure 7. Overview of packet routing within the VANET.

creation process (see Figure 7).

The Care-of Route discovery and validation signalling is repeated periodically, both to refresh the ad-hoc routes and to avoid time-shifting attacks. If an ad-hoc route becomes invalid (for example, because it expires) or it is broken, and traffic is received through this route, a *Care-of Route Error* (CoRE) message is sent (and forwarded) by each MR in the path to the source MR. For example, if intermediate MR Y in Figure 7 receives data traffic from MR A addressed to MR B and the link between MR Y and the next hop towards MR B (in this case, MR B itself) is broken, then MR Y sends a CoRE message to the next MR along the path towards the source MR (MR A), which is MR X, indicating that there is a problem with this Care-of Route:

$$Y \rightarrow X:$$
$$[\mathbf{CoRE}, HoA_A, HoA_B, N_Y, K_{Y+}]_{K_{Y-}}$$

This message is received by MR X, which after verifying the authenticity of the received CoRE, signs the message, adds its public key K_{X+} and the signature to the message (as performed by intermediate MRs when processing and forwarding CoRTI and CoRT messages) and sends it to the next hop towards MR A.

$$Y \rightarrow X:$$
$$\left[[\mathbf{CoRE}, HoA_A, HoA_B, N_Y, K_{Y+}]_{K_{Y-}}, K_{X+}\right]_{K_{X-}}$$

Upon reception of this error message, the source MR (MR A in the example) switches to use the Home Route for sending packets and it may start a new route

discovery procedure to set-up a new optimised Care-of Route within the VANET. To avoid DoS attacks, a CoRE message indicating that a route has become invalid is only processed by an MR if the neighbour that is forwarding the message is the next hop of this route. Otherwise, malicious nodes would be able to set as invalid any Care-of Route.

There exist several possible mechanisms that can be used to detect that a Care-of Route is no longer working. As an example, Mobile Routers may check if the data packets forwarded within the VANET have been correctly received by the next hop making use of link layer acknowledgement frames (if the MAC layer supports that). If several data frames have not been acknowledged, this may be used as an indication that the next hop is no longer reachable and therefore the Care-of Route is broken.

4.3 Security Analysis

A malicious node M could attempt several attacks to this scheme. Basically, there are two main types of attacks: those that try to modify the routing in the VANET, and those that try to steal a prefix. In order to modify the ad-hoc routing, an attacker out of the routing path could try to alter or fabricate routing messages. Such kind of attack is not feasible because all routing messages are cryptographically signed. An additional attack could be to try to impersonate a legitimate node (spoofing its IP address), but this is not possible either, since the authenticity of a message is guaranteed by the use of CGAs and public key cryptography. Two possible examples of these attacks are described next.

A malicious node M can try to change an already established ad-hoc route by sending a CoRTI message to an MR X that belongs to this multi-hop route, claiming that M can reach a certain MR A. But X will not accept the message if it cannot validate it with the public key corresponding to the HoA of MR A associated with the route. Because M cannot create that part of the CoRTI message, it can try to copy it from a real CoRTI message previously sent by MR A, but the nonce included will not be greater than the one stored in MR X that is associated with the route. Notice that a legitimate update of the route by MR A is allowed because it knows its own private key and the nonce that must be included in the CoRTI message.

A malicious node M that receives a CoRTI message from an MR A could try to claim to a neighbour MR X that it is MR Z and not M (when sending the CoRTI message towards MR B). If MR Z is a legitimate network node, this could mean that afterwards all the traffic will be sent to it (DoS attack). But M will not be able to do that because it does not have the private key associated with the HoA that MR Z is using.

One example of an attack based on spoofing a prefix will be as follows. A malicious

node M could create a HoA belonging to the MNP managed by a legitimate MR A. The node M can create the HoA belonging to the MNP of MR A using its own public key so it can prove to other nodes that it has the private key corresponding to that address. However, the Home Route Test will fail, so it cannot make another MR send to it the traffic addressed to the MNP of MR A. In this situation, the node M can set-up an ad-hoc route for its HoA (using its own private key), since the routes created in the VANET only define the forwarding of packets addressed to MRs' HoAs (see Figure 7). Therefore, different routes for HoAs belonging to the same prefix could coexist (although only one at most will belong to non-malicious nodes). However, only legitimate end-point MRs will success in performing the Home Route Test and, therefore, will be able to generate and send a valid MNPBU (enabling the use of the Care-of Route). Notice that packets sent to a legitimate IP address equal to a HoA used by a malicious node to create an ad-hoc route, will reach the intended destination because they will traverse the ad-hoc network encapsulated inside a tunnel with the legitimate HoA.

There are some vulnerabilities and attacks that are still possible, resulting from the inherent nature of ad-hoc networks, such as certain Denial-of Service (DoS) – e.g., based on non-collaborating nodes – or route discovery flooding attacks. But, notice that VARON nodes can always revert communications to the Home Route in case of the Care-of Route is not working.

5 Performance of VARON

In order to complete our discussion about the proposed solution, an extensive simulation study was performed. Besides analysing the performance and costs of VARON, the value of some metrics using VARON are compared to the ones obtained when plain NEMO Basic Support protocol [5] or MIRON [11] (as an example of a non ad-hoc Route Optimisation for NEMO) were used.

5.1 Computational cost

Each VARON Mobile Router must perform several cryptographic operations (such as signing and verifying signatures) on each signalling message along a Care-of Route. These cryptographic operations are relatively expensive, especially when compared to the operation of the NEMO Basic Support protocol and other (insecure) ad hoc routing protocols, that do very little (almost negligible) computation per signalling message. However, it is important to note that only the routing control messages that make the state of the MR change or the MR perform an action (e.g., modifying the routing table, forwarding a message, etc.) are subject to signing/verifying. The signature of those routing messages that are discarded (e.g.,

because they have been already processed and are received again forwarded by a different MR) is not verified. Data packets exchanged between nodes after a route has been set up are not processed by VARON either.

In order to evaluate the computational cost of VARON, several tests were conducted, measuring the raw processing time expended on each of the operations performed when processing VARON routing packets for different key sizes. The cryptographic functions were implemented making use of the OpenSSL Library [12] , which provides functions for general purpose cryptographic tasks such as public and private key encryption/decryption and signature creation/verification. The measurements were conducted in two different types of devices that are likely to play the role of a vehicular Mobile Router: a Linksys WRT54GS router (which is a small home and office broadband router, equipped with a 200 MHz processor, an IEEE 802.11g WLAN interface and an IEEE 802.3 Ethernet interface connected to a VLAN capable 5-port switch) and a laptop (Intel Core-duo 2.0 GHz with 2 GB RAM).

The processing performed by an MR on VARON control packets is composed of some of the following operations (depending on the VARON message, not all of them are performed on each packet):

- **CGA verif.:** Verification of the CGA. If the message has been forwarded by an intermediate MR, the CGAs of both the original sender and the forwarder have to be checked.
- **Sign. verif. 1:** Verification of the signature of the sender MR.
- **Sign. verif. 2:** Verification of the signature of the forwarder MR (in case of the message has been forwarded by an intermediate MR).
- **Sign. comp. 1:** Computation of the signature by the sender MR when a new message is generated (e.g., a CoRTI/CoRT message).
- **Sign. comp. 2:** Computation of the signature by an intermediate MR when a message has to be forwarded (e.g., a CoRTI/CoRT message).

Table 2 shows the results for each of the cryptographic operations that are involved in the processing of VARON routing messages. The processing time for the laptop and the Linksys router were measured over three different RSA key sizes: 512, 768, and 1024 bits. For both devices, an increase in the key size of 256 bits results in approximately doubling the signature computation processing. The time required to verify a signature or a CGA is almost negligible compared to the time required to compute signatures, as expected, because of the nature of public key cryptography. It is also interesting, although not very surprising, the difference in processing times between the laptop and the Linksys router. For each key size, the processing time is between 10 and 20 times slower on the router than on the laptop. The results obtained for the Linksys router for the 1024-bit RSA key have been used as input

[12] `http://www.openssl.org/`

RSA key size (bits)	Average ± Std. Dev. (ms)				
	CGA verif.	Sign. verif. 1	Sign. verif. 2	Sign. comp. 1	Sign. comp. 2
Laptop					
512	0.47 ± 0.05	0.42 ± 0.05	0.40 ± 0.02	2.36 ± 0.09	2.46 ± 0.20
768	0.47 ± 0.02	0.52 ± 0.04	0.52 ± 0.01	5.09 ± 0.16	5.13 ± 0.43
1024	0.59 ± 0.16	0.87 ± 0.05	0.89 ± 0.09	12.03 ± 0.27	11.94 ± 0.36
Linksys					
512	13.58 ± 0.07	11.06 ± 0.06	11.08 ± 0.07	45.90 ± 0.37	45.86 ± 0.28
768	14.08 ± 0.93	12.72 ± 0.71	12.57 ± 0.43	79.86 ± 0.78	80.64 ± 1.31
1024	13.73 ± 0.38	14.47 ± 0.06	14.52 ± 0.08	136.61 ± 0.41	136.66 ± 0.44

Table 2
Raw time required to perform the cryptographic operations required when processing VARON signalling packets.

to the simulations described in the next section. This will provide us with more realistic results (that can be considered as a lower bound on the performance if more powerful devices were used instead).

5.2 Simulation of VARON

We performed our simulations using OPNET [13] . We simulated 50 vehicles within a road. Each vehicular MR is equipped, in addition to the ingress interface (to provide connectivity to the vehicular devices), with an emulated UMTS egress interface (1 Mbit/s, 150 ms of average one-way delay) and an IEEE 802.11 (WLAN) interface (2 Mbit/s, transmission power of 1 mW, receiver sensitivity of -95 dBm) in ad-hoc mode. The UMTS interface has been emulated because OPNET UMTS models did not properly support IPv6 at the time of performing the simulations. The UMTS channel has been modelled using a 1 Mbit/s WLAN 802.11b network, with an additional delay of 150 ms per way. The link delay has been chosen based on previous practical measurements [19], [20], [21]. In order to achieve global coverage, the transmission power of the WLAN nodes (MRs and the Access Point) that emulates the UMTS was set to 1 W. Considering the kind of analysis that we were interested in performing, this set-up provided us with a reasonable model of a UMTS network.

The UMTS interface provides continuous Internet connectivity, whereas the WLAN interface enables forming multi-hop vehicular ad-hoc networks. UMTS and WLAN

[13] OPNET University Program, `http://www.opnet.com/services/university/`

were chosen for the simulations because they are probably the most realistic candidate access technologies for a vehicular communication scenario nowadays. However, different technologies may also be used by VARON (e.g., IEEE 802.16e WiMAX for the MR's egress interface), since the protocol is independent of the access technology used by the Mobile Router.

In order to evaluate the worst case scenario, VARON was simulated using 1024 bit RSA keys and the processing time results shown in Table 2 for the Linksys router as input for the simulations. All the VARON protocol, but the detection of broken links and the generation of CoRE messages, was implemented using the OPNET simulator [14] . By not implementing the detection of broken routes, a Care-of Route entry can only be removed from the IP routing table of an MR when it expires [15] . Hence, it may happen that an MR tries to use a broken Care-of Route for some time (until it expires), since MRs along the path are not able to detect a broken route and therefore they do not send any CoRE message to the source MR – that would make it stop sending the traffic through the VANET and revert to use the Home Route. Thus, VARON performance obtained from the simulation results is worse than the one that would be obtained if the protocol were completely implemented.

A random delay uniformly distributed between 0 and 1 second was added before forwarding a HoAA message in order to minimise collisions. This random delay was introduced because it was observed that the performance when HoAA messages were forwarded immediately after their reception was quite poor. This is related to the 802.11 MAC protocol, which does not perform a ready-to-send/clear-to-send (RTS/CTS) exchange for broadcast packets, and therefore does not prevent high probabilities of collision of broadcast packets from appearing in relatively dense networks such as the simulated one (50 nodes).

In order to evaluate the performance of VARON under different real-case scenarios, VARON experiments were performed varying the following two parameters:

a) *Vehicle speed.* Different simulations were run for average vehicle speeds of 1, 5, 10, 20, 40, 50, 70, 90, 100 and 120 [16] km/h. The speed of a node is a random variable, uniformly distributed between $0.9v$ and $1.1v$, where v is one of the previous mean speed values. Therefore, in each simulation, nodes have different speeds, but still very similar. This represents real life scenarios, such as vehicles in a city or motorway, where the relative speed of vehicles moving in the same direction is low.

[14] VARON model has approximately 10000 lines of code.
[15] In the simulations, Care-of routes were marked as *expired* after 20 seconds. Expired Care-of routes are not kept in the IP routing table for 10 additional seconds, so there is enough time for the Mobile Router to refresh the Care-of Route (in case there is data traffic being delivered using this route). These values were chosen after performing several sets of simulations aimed at finding good values for these parameters.
[16] The maximum speed limit in Spain is 120 km/h.

b) *Initial vehicle density.* Different simulations were run for initial vehicle densities of 200, 100, 50, 25, 20, 13.33, 10, 8, 6.67, 5, 4 and 3.33 vehicles/km [17] .

For each combination of the previous parameters, thirty different simulations were performed, changing the speeds and initial positions of the vehicles, as well as the seed of the random number generator of the simulator. The following metrics were evaluated:

(1) **Average end-to-end throughput.** This is the mean TCP throughput obtained when performing bulk file transfers. This evaluates the improvement in terms of throughput obtained when using VARON, as well as the possible effects that the use of VARON may have in TCP (e.g., due to the Home ↔ Care-of Route handovers).
(2) **Average Care-of Route acquisition latency.** This is the average delay between the sending of a Care-of Route Test Init packet by an originator MR for discovering and establishing a Care-of Route to a target MR, and the receipt of the Mobile Network Prefix Binding Update message that makes the MR add a Care-of Route entry to its IP routing table. This includes the delays of the signalling messages sent through the VANET (CoRTI, CoRT and MNPBU), the processing time due to the cryptographic operations performed on each routing message and the delay due to the use of the infrastructure (Home Route) to send HoRT messages.
(3) **Average Care-of Route length.** This is the average length of the Care-of Route discovered and set-up by VARON. It is calculated by averaging the number of hops taken by MNPBU messages to reach their destination (the path followed by an MNPBU message is the same that the one that data packets sent through the VANET would follow afterwards).
(4) **Average frequency of route changes.** This is the average number of Home ↔ Care-of Route changes per minute. This evaluates the stability of the Care-of routes discovered by VARON.
(5) **Average Care-of Route data packet fraction.** This is the fraction of delivered data packets that are sent through a Care-of Route. This evaluates the fraction of data traffic that is actually forwarded through an optimised route, and therefore the likelihood of using VARON to optimise a traffic communication between two vehicles that are relatively close each other.
(6) **Average VARON signalling load (bytes).** This is the ratio of overhead bytes to delivered data bytes using a Care-of Route. This metric was measured counting the amount of VARON signalling bytes received at a Mobile Router and the amount of data bytes received through the Care-of Route (data packets received through the Home Route were not taken into account for this calculation).

[17] This means that at the beginning of each simulation, the 50 nodes were uniformly distributed within a road of a length of 0.25, 0.5, 1, 2, 2.5, 3.75, 5, 6.25, 7.5, 10, 12.5 and 15 km, respectively, and then they started to move at their respective speeds.

(7) **Average VARON signalling load (packets).** Similar to the previous metric, but a ratio of signalling packets to data packets overhead.

On each simulation only two nodes out of the 50 were communicating each other. Simulations involving more nodes communicating simultaneously were also performed to validate the correct operation of the solution. The throughput and signalling load metrics were obtained simulating a scenario in which a 2 MByte file is transferred from a vehicle to another, using FTP. For the rest of the metrics, the scenario consisted of a UDP VoIP flow (GSM, 24.2 kbit/s, 50 packets per second) sent from a vehicle to another.

To simulate the delay added by the use of the NEMO Basic Support protocol [5] and the traversal of the respective Home Networks of the involved vehicles, an additional delay (one-way) of 36 ms was introduced in the infrastructure network. This additional latency represents the delay required to go through two Home Networks located in Europe (the value was chosen based on real RTT measurements [18] obtained from the PingER project [22]).

5.3 Simulation results

Simulation results are presented next in Figures 8-13. Results are plotted using three-dimensional graphs, so the impact of the vehicle density and speed on each of the simulated metrics can be easily evaluated. Each data point is an average of thirty simulations run with different randomly generated mobility patterns (but following the considerations described above about speed and movement within a road).

Figure 8 shows the average route acquisition latency, that is the time taken by VARON to find and set-up a Care-of Route. VARON requires each MR along the path to perform several cryptographic operations when processing a control packet, such as the verification and generation of digital signatures and CGAs. This is computationally demanding and therefore adds additional delay to the overall route acquisition time. Another source of latency in the route acquisition time is the use of the infrastructure network (i.e. Home Route) in the Care-of Route validation process, that causes an additional delay – equal to the sum of the RTTs of each MR to its respective HA – in the Care-of Route discovery time. Therefore, the route acquisition time is higher in VARON than in other ad-hoc routing protocols, although in VARON this time does not have a direct impact on normal data packet forwarding, as data traffic delivery is guaranteed by the use of the Home Route. Since an important contribution to the overall route acquisition time comes from the cryptographic operations performed on each hop, this time is higher when the vehicle density decreases, because in a less populated VANET, the average number

[18] Available at `http://www-iepm.slac.stanford.edu/pinger/`

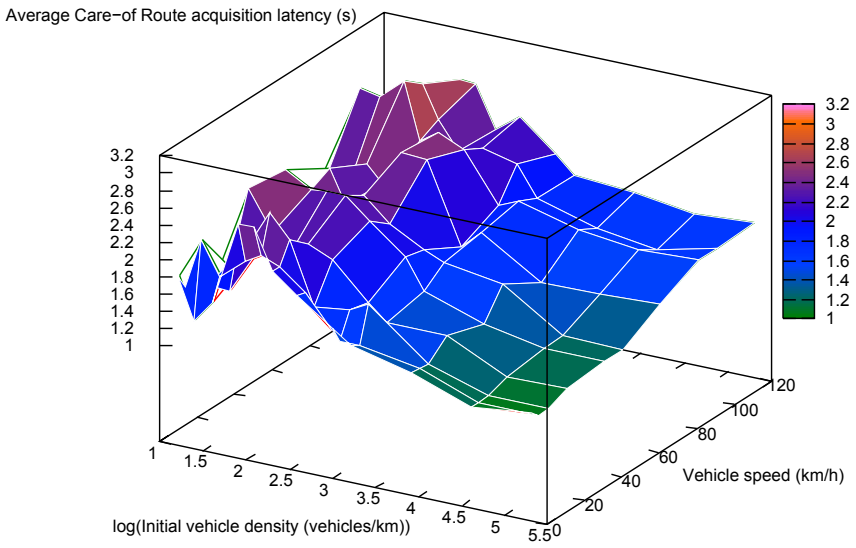


Figure 8. Average Care-of Route acquisition latency.

of intermediate MRs involved in a communication is higher (this will be shown later in Figure 9). However, if the average distance between vehicles is too high (that is, the vehicle density is quite low), this may lead to the situation where only direct 1-hop communications are possible (this explains why the route acquisition time decreases for very low vehicle densities).

Vehicle speed has also an effect on the Care-of Route acquisition time – although this effect is minor than the vehicle density – especially in highly populated scenarios. This effect is caused by the fact that it is more likely that more intermediate nodes are required to participate in the Care-of Route in high speed scenarios, since the distance between two vehicles that are communicating increases (because the relative speed of the vehicles is higher than in low mobility scenarios [19]).

Figure 9 shows the average Care-of Route length. The results shown in this graph basically confirm what has been discussed in the previous paragraph, that is, the strong dependency that the route acquisition time has on the number of hops of the Care-of Route. Since the delay caused by the HoRT messages traversing the infrastructure is the same for each route, independently of its length, the cost of performing cryptographic operations on each hop is an important factor in the route acquisition time. Obtained results show that for highly populated scenarios, two MRs within the VANET are able to communicate directly almost always. For very low populated scenarios, the average number of hops of a Care-of Route decreases,

[19] It should be recalled that in the simulations each vehicle moves with a constant velocity, which is a random variable uniformly distributed between $0.9v$ and $1.1v$ (the mean speed, v, is varied from from 1 to 120 km/h). This causes that in those scenarios where the mean speed (v) is higher, the relative speed of two moving vehicles will be also higher. For example, if v is 120 km/h, the speed of each vehicle is uniformly distributed between 108 and 132 km/h, so the relative velocity of two vehicles may be up to 24 km/h.

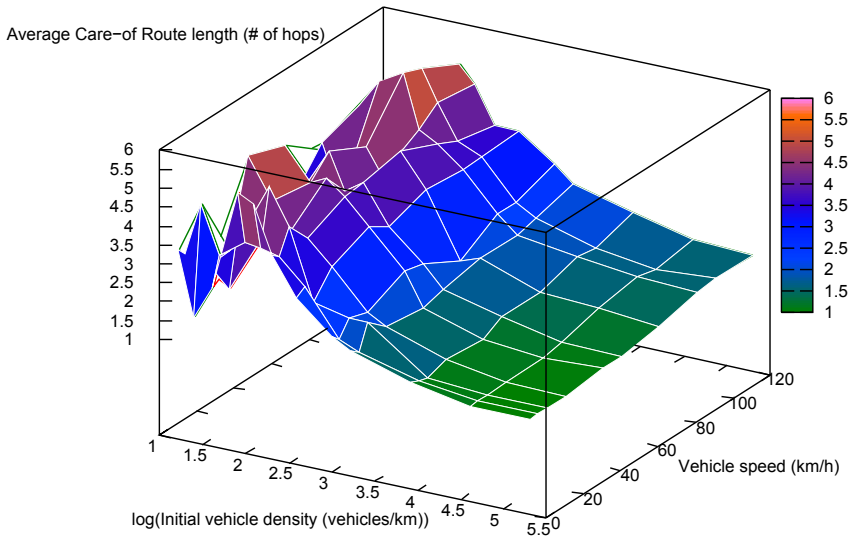


Figure 9. Average Care-of Route length.

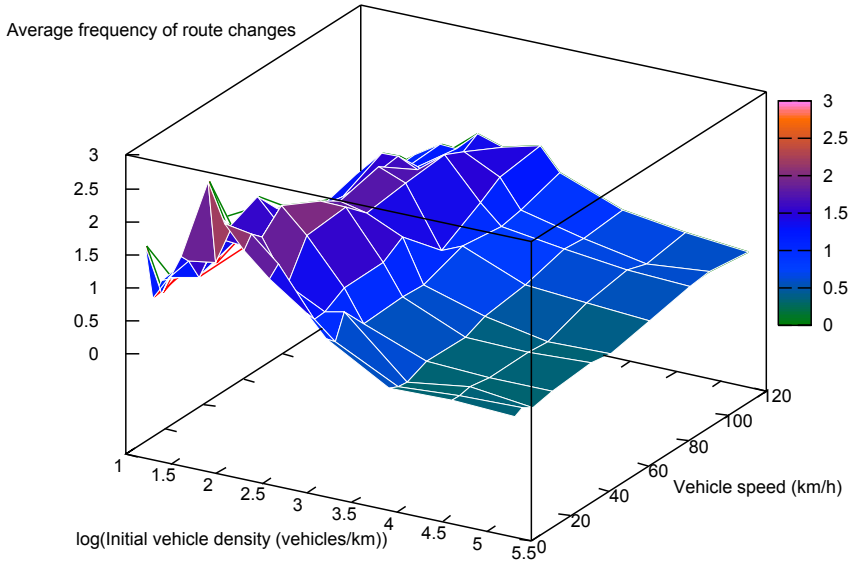


Figure 10. Average frequency of route changes.

since it is more difficult to establish a route within the VANET, unless the two MRs can communicate directly. Vehicle speed also has an impact on the length of the route, at faster speeds the Care-of Route length increases (the reason for that is the same that the one for the increment in the acquisition time explained above).

From the obtained average number of hops involved in a Care-of Route, it may be deduced that VARON, although it is not designed to explicitly find the shortest path in terms of number of hops, usually finds the shortest route, since the first CoRTI received at the target MR normally travels along the shortest path (this may not be true in situations of network congestion, where the fastest path may not be the shortest). Therefore, VARON seems to perform well at finding the shortest Care-of Route.

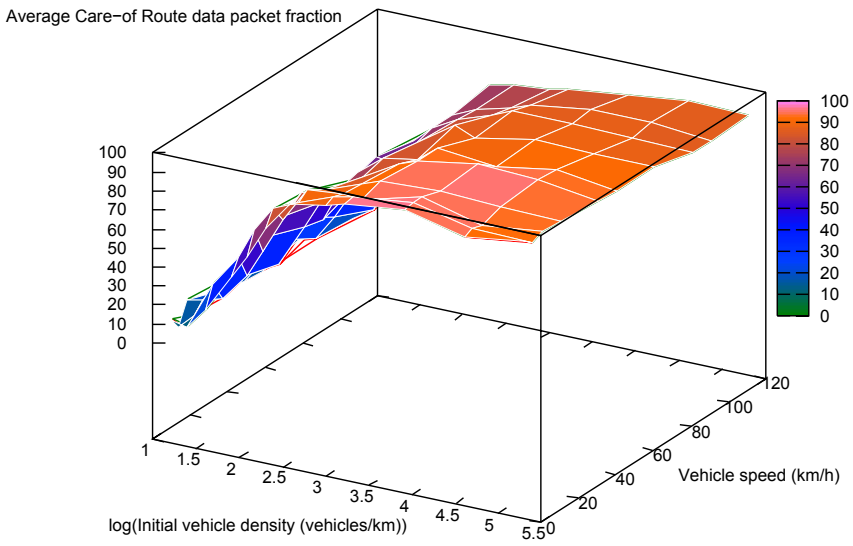


Figure 11. Average Care-of Route data packet fraction.

Figure 10 shows the average frequency of route changes, that is the number of times during the lifetime of a communication flow that the route used to forward the packets switches from a Care-of Route to the Home Route, and vice-versa. This metric is important in order to evaluate the stability of the optimised Care-of routes. Obtained results show that the frequency of route changes grows when the vehicle density decreases, which is an expected behaviour, since in highly populated scenarios the Care-of Route average length is small, so it is less probable that the route changes because there are less involved MRs. In very low populated scenarios, the frequency of route changes decreases, because it is less likely that a Care-of Route can be established and used, and therefore the number of route changes is smaller (i.e. most of the times traffic is forwarded through the Home Route).

Figure 11 shows the average Care-of Route data packet fraction, which is the fraction of delivered packets that are received through a Care-of Route. Therefore, this metric represents the likelihood of optimising the traffic by using the VANET. Obtained results show that there are more opportunities of optimising a communication in high populated scenarios and that the speed have also a small effect on the probability of establishing a Care-of Route (in highly mobile scenarios the probability is lower). This result is also expected, since in those situations where a small number of hops is required to communicate two MRs, it is easier to set-up a Care-of Route, which is, moreover, more stable.

Figure 12 shows the average end-to-end TCP throughput obtained results [20] . In order to compare the performance obtained by VARON with other approaches, the

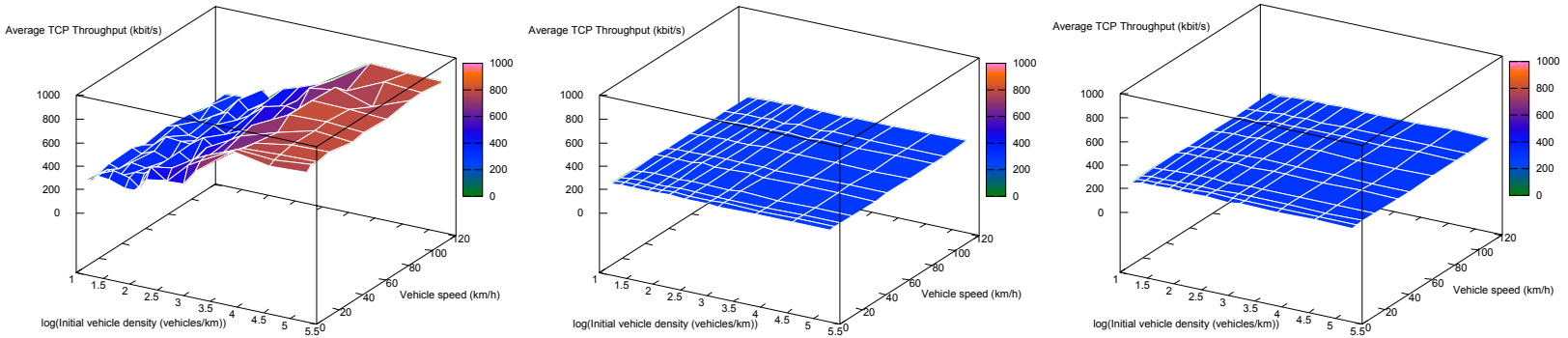
[20] In the experiments, the following configuration was used on the nodes: a TCP receive buffer size of 87380 bytes and the TCP Window Scale option enabled. This represents a standard TCP configuration nowadays (this is the default configuration of a Linux-2.6 machine).

TCP throughput obtained with the NEMO Basic Support protocol and MIRON are also shown. Figure 12(a) shows the results when VARON is enabled in the vehicles. The TCP throughput decreases with decreasing vehicle density, since in scenarios with low population of vehicles, it is harder to set-up a Care-of Route, longer paths (see Figure 9) are usually required, and the configured routes have short lifetimes (see Figure 10). As it was shown in Figure 11, this leads to a low fraction of data traffic being sent through the VANET, and therefore the overall performance is poor. Besides, the fact of not having implemented the detection of broken routes has also an impact on the obtained TCP throughput, since the packet loss – that may be experienced when a route breaks until it is deleted from the IP routing table (after its expiration) – makes TCP congestion protocol reduce its transmission rate [21]. Actually, for very low vehicle densities, the performance obtained with the NEMO Basic Support protocol (approximately 275 kbit/s, as shown in Figure 12(b)) or MIRON (approximately 300 kbit/s, as shown in Figure 12(c)) is better than with VARON. However, obtained results show that for scenarios not so low populated – as urban or even inter-urban scenarios, where vehicles are typically distributed within roads with inter-vehicle distances of less than 150 m – VARON outperforms both NEMO Basic Support protocol and MIRON. For high vehicle densities (e.g., traffic jams), the TCP throughput obtained with VARON is close to 1 Mbit/s, which is a great improvement over the non vehicular optimised protocols (NEMO and MIRON). This improvement is provided by VARON because of two main reasons:

- VARON enables the use of a VANET network built using an access technology – such as IEEE 802.11 – that typically has more bandwidth that the access technology used by a vehicle to connect to the Internet (e.g., GPRS/UMTS).
- VARON enables direct data packet forwarding within the VANET, avoiding to use the infrastructure network and therefore reducing drastically the end-to-end delay. Since TCP performance is heavily dependent on the round trip time (RTT) between the communication peers, this end-to-end delay reduction contributes to the TCP throughput improvement.

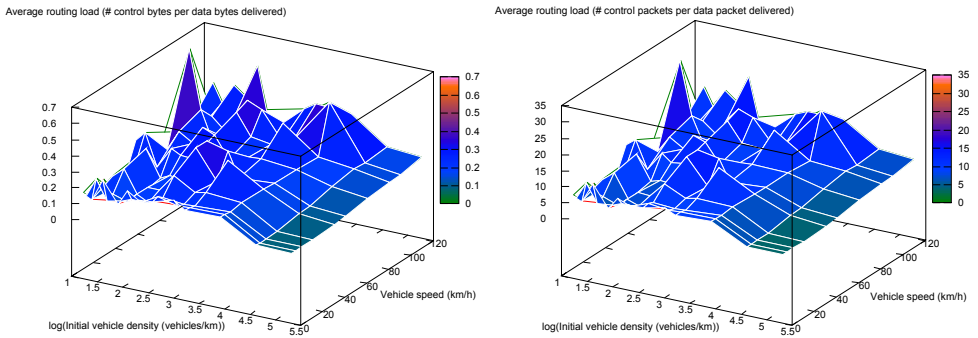
The last simulated metric was the signalling load introduced by VARON. Figure 13 shows the signalling load, measured both in bytes and packets. Obtained results show that the overhead introduced by VARON, because of periodic HoAA messages and the Care-of Route discovery, is not negligible. VARON's byte signalling load (shown in Figure 13(a)) reaches almost 70% in low populated and high speed scenarios, although it is about 20% for the rest of the scenarios (e.g., urban and inter-urban). Results show that there is a constant amount of overhead caused by the periodic HoAA flooding, but the main contribution to this overhead comes from the Care-of Route discovery and set-up signalling.

[21] The retransmission threshold behaviour used in the simulations was configured according to the TCP standard and ensuring that connections could not break because of excessive retransmission attempts.



(a) VARON (b) NEMO (c) MIRON

Figure 12. Average end-to-end TCP throughput (standard TCP configuration).



(a) (bytes) (b) (packets)

Figure 13. Average VARON signalling.

Although VARON's byte signalling is not negligible, it is relatively low in most of the scenarios. VARON's packet overhead (shown in Figure 13(b)) results show that VARON requires a great amount of small signalling packets to work (the number of received VARON signalling packets even reaches 35 times the number of data packets in the worst case scenario). This is caused by the periodic HoAA flooding and also by the flooding nature of the Care-of Route discovery signalling. Besides, the same signalling is required periodically to refresh an already established route.

VARON's overhead may seem to be very high and therefore it may be argued that it is not a good optimisation mechanism. However, there are several considerations that should be taken into account:

- Almost all the signalling required by VARON is sent through the ad-hoc interface. This interface is not used to send non optimised regular traffic and it has typically no cost associated. It may be argued that sending so many packets imposes a non negligible energy cost, but in vehicles this cost is not so important, since they have a powerful and rechargeable source of energy. On the other hand, the computational cost associated to sending this signalling may have an impact on the overall performance of the Mobile Router. Simulations have taken into account the cost associated to the cryptographic computations performed on each packet, but forwarding a packet has also a cost, that depending on the MR's capabilities may be relevant.
- The VARON simulated model does not implement the detection of broken links and the CoRE associated signalling. By implementing this missing part, other configuration parameters – such as the periodic timers involved in the Care-of Route discovery and refreshment – could be set to less aggressive values (in terms of periodicity and, therefore, associated overhead). The refreshment of a Care-of Route – through periodic CoRTI/CoRT signalling – could even be removed if the algorithm followed to detect broken links is good enough and ensures that all broken links can be detected. If not, it could always be optimised, for example by not re-doing the full Care-of Route discovery process (that involves a partial flooding of the VANET), but just sending a probe packet through the established Care-of Route to check if it is still working.

Although graphs only display average values for the different simulated metrics, the normalised standard deviation has also been calculated. Obtained results show that the normalised standard deviation is higher in the low populated and high mobile scenarios than in the high populated and low mobile scenarios, meaning that former scenarios are more unstable than the latter ones.

One important conclusion that can be drawn from the simulation work is that in highly mobile and low populated scenarios, it is more difficult to set-up a multi-hop route between two vehicles, mainly because of the instability in the ad-hoc routing. Therefore, most of the chances of communication involve routes with a very low number of hops. An example of communication scenario that will greatly

benefit from VARON optimisations would be that of military convoys or emergency service operations, where a group of vehicles move together.

6 Conclusions

In this paper we have analysed the problem of enabling communications from and between vehicles. A first step is the provision of connectivity to the Internet. Cars will likely have specialised devices (Mobile Routers) that will provide network access to the rest of the devices in the car, i.e. the car will contain a Mobile Network. For this reason we propose the application of Network Mobility solutions to this scenario. The NEMO Basic Support protocol is the straightforward option. The performance limitations of this scenario can be partially overcome through the application of a NEMO Route Optimisation solution.

In this paper we have proposed VARON, a solution that enables optimal direct vehicle-to-vehicle communication, using an ad-hoc network. VARON benefits from the simultaneous reachability of vehicles through the infrastructure and the ad-hoc network to secure the communications in the ad-hoc part. Although the proposed solution does not preclude the possibility of performing some Denial of Service attacks, that are inherent to the ad-hoc environment, these attacks only affect the ad-hoc route and the vehicles can always fall back on the communication through the infrastructure if needed. The benefit of the proposed mechanism is a clear improvement in end-to-end throughput and delay with security guarantees similar to those available in infrastructure communications.

The proposed protocol has been validated and evaluated through extensive simulation conducted with OPNET. Results show that VARON improves significantly the performance in terms of TCP throughput when compared to other approaches such as the use of plain NEMO Basic Support protocol or a generic Route Optimisation solution for NEMO – such as MIRON – not suited for vehicular environments in which cars obtain Internet access from low-bandwidth and high-delay access technology (e.g., GPRS/UMTS). Simulation has also shown that in highly mobile and low populated scenarios, the probability of using the VANET to route traffic is low, because of the instability in the ad-hoc routing. Most of the opportunities of optimised communication involve routes with a very low number of hops (less than 5 hops). Hence, scenarios such as urban and inter-urban communications (e.g., traffic jams, vehicles in a motorway) may greatly benefit from deploying VARON, especially in the case of a group of vehicles moving together, such as military convoys or emergency service operations. On the other hand, it is not worth using VARON in highly mobile and low populated scenarios – such as highways – since the probability of optimising a communication is very low and its lifetime would be very short.

Although the paper has presented VARON as a solution suited for vehicular environments, its applicability is not limited to that scenario. Actually, any scenarios involving mobile networks that are able to set-up an ad-hoc network, are good candidates for VARON deployment. For example, passengers on a train carrying their Personal Area Networks (PANs) may be using peer-to-peer file sharing or Instant Messaging (IM) applications while travelling (e.g., by using a PDA or laptop connected to a mobile phone with 3G and WLAN capabilities acting as the Mobile Router). If the two users involved in the peer-to-peer communication are located within the same train, their MRs may decide to bypass the routing infrastructure and directly send their traffic using a direct ad-hoc communication.

An interesting issue that we have not analysed in this paper is the applicability of VARON to provide Route Optimisation in nested NEMO scenarios. Additionally, when VARON is not used in vehicular environments, the power consumption of the solution may be an issue, and therefore it is interesting to study how VARON performs in battery-limited environments. We are currently working on both topics in order to understand if VARON applicability can be also extended to these two scenarios.

Acknowledgement

We would like to thank Marcelo Bagnulo, Alberto García-Martínez and Manuel Urueña for their helpful comments that contributed to improve VARON design.

References

[1] W. Kellerer, C. Bettstetter, C. Schwingenschlogl, P. Sties, K.-E. Steinberg, H.-J. Vögel, (Auto) Mobile Communication in a Heterogeneous and Converged World, IEEE Personal Communications 8 (6) (2001) 41–47.

[2] O. Andrisano, R. Verdone, M. Nakagawa, Intelligent transportation systems: the role of third generation mobile radio networks, IEEE Communications Magazine 38 (9) (2000) 144–151.

[3] J. Ott, D. Kutscher, The ”Drive-thru” Architecture: WLAN-based Internet Access on the Road, in: IEEE Vehicular Technology Conference (VTC), Vol. 5, 2004, pp. 2615–2622.

[4] H.-Y. Lach, C. Janneteau, A. Petrescu, Network Mobility in Beyond-3G, IEEE Communications Magazine 41 (7) (2003) 52–57.

[5] V. Devarapalli, R. Wakikawa, A. Petrescu, P. Thubert, Network Mobility (NEMO) Basic Support Protocol, Internet Engineering Task Force, RFC 3963 (Proposed Standard) (January 2005).

[6] D. Johnson, C. Perkins, J. Arkko, Mobility Support in IPv6, Internet Engineering Task Force, RFC 3775 (Proposed Standard) (June 2004).

[7] T. Ernst, Network Mobility Support Goals and Requirements, Internet Engineering Task Force, draft-ietf-nemo-requirements-06.txt (work-in-progress) (November 2006).

[8] C.-W. Ng, P. Thubert, M. Watari, F. Zhao, Network Mobility Route Optimization Problem Statement, Internet Engineering Task Force, draft-ietf-nemo-ro-problem-statement-03.txt (work-in-progress) (September 2006).

[9] C.-W. Ng, F. Zhao, M. Watari, P. Thubert, Network Mobility Route Optimization Solution Space Analysis, Internet Engineering Task Force, draft-ietf-nemo-ro-space-analysis-03.txt (work-in-progress) (September 2006).

[10] E. Perera, V. Sivaraman, A. Seneviratne, Survey on Network Mobility Support, ACM SIGMOBILE Mobile Computing and Communications Review 8 (2) (2004) 7–19.

[11] M. Calderón, C. J. Bernardos, M. Bagnulo, I. Soto, A. de la Oliva, Design and Experimental Evaluation of a Route Optimisation Solution for NEMO, IEEE Journal on Selected Areas in Communications 24 (9) (2006) 1702–1716.

[12] D. Forsberg, Y. Ohba, B. Patil, H. Tschofenig, A. Yegin, Protocol for Carrying Authentication for Network Access (PANA), Internet Engineering Task Force, draft-ietf-pana-pana-11.txt (work-in-progress) (March 2006).

[13] R. Droms, J. Bound, B. Volz, T. Lemon, C. E. Perkins, M. Carney, Dynamic Host Configuration Protocol for IPv6 (DHCPv6), Internet Engineering Task Force, RFC 3315 (Proposed Standard) (July 2003).

[14] R. Wakikawa, H. Matsutani, R. Koodli, A. Nilsson, J. Murai, Mobile Gateways for Mobile Ad-Hoc Networks with Network Mobility Support, in: Proceedings of 4th International Conference on Networking (ICN), 2005, pp. 361–368.

[15] P. Nikander, J. Arkko, T. Aura, G. Montenegro, E. Nordmark, Mobile IP Version 6 Route Optimization Security Design Background, Internet Engineering Task Force, RFC 4225 (Informational) (December 2005).

[16] K. Sanzgiri, D. LaFlamme, B. Dahill, B. N. Levine, C. Shields, E. M. Belding-Royer, Authenticated Routing for Ad Hoc Networks, IEEE Journal On Selected Areas In Communications 23 (3) (2005) 598–610.

[17] T. Aura, Cryptographically Generated Addresses (CGA), Internet Engineering Task Force, RFC 3972 (Proposed Standard) (March 2005).

[18] C. Ng, J. Hirano, Extending Return Routability Procedure for Network Prefix (RRNP), Internet Engineering Task Force, draft-ng-nemo-rrnp-00.txt (work-in-progress) (October 2004).

[19] T. Melia, A. de la Oliva, I. Soto, C. J. Bernardos, A. Vidal, Analysis of the effect of mobile terminal speed on WLAN/3G vertical handovers, in: Proceedings of the 2006 IEEE Global Telecommunications Conference (GLOBECOM), San Francisco, California (USA), 2006.

[20] A. D. L. Oliva, T. Melia, A. Vidal, C. J. Bernardos, I. Soto, A. Banchs, A case study: IEEE 802.21 enabled mobile terminals for optimised WLAN/3G handovers, Mobile Computing and Communications Review (accepted to appear).

[21] P. Vidales, C. J. Bernardos, I. Soto, D. Cottingham, J. Baliosian, J. Crowcroft, MIPv6 Experimental Evaluation using Overlay Networks, Computer Networks (accepted to appear).

[22] W. Matthews, L. Cottrell, The PingER project: active Internet performance monitoring for the HENP community, IEEE Communications Magazine 38 (5) (2000) 130–136.