Extending DNS to Support Geocasting Towards VANETs: A Proposal

Tiago Fioreze and Geert Heijenk

University of Twente

Centre for Telematics and Information Technology (CTIT)

Faculty of Electrical Engineering, Mathematics and Computer Science (EEMCS)

Department of Design and Analysis of Communication Systems (DACS)

Enschede, The Netherlands

{t.fioreze,geert.heijenk}@utwente.nl

Abstract—The delivery of IP packets to a set of elements lying within a designated geographical area, also known as geocasting, is an important aspect in vehicular networks. Geocast messages can be used, for instance, to warn drivers about road conditions (e.g., weather hazards) and therefore prevent accidents. In order for geocasting to work on the Internet, IP addresses must be associated with geographical coordinates, either temporary (vehicles in transit on a road) or permanently (roadside units along the road). However, finding IP nodes within specified geographical areas is still an open issue, even though several proposals have been made. The objective of this paper is to introduce a novel proposal to extend DNS capabilities in order to support geocast.

I. INTRODUCTION

Transport infrastructures and vehicles are moving more and more towards intelligent systems. Intelligent Transportation Systems (ITS) [1] envisage information to be shared among vehicles, and between vehicles and roadside units through wireless communications technology to make transportation safer and more comfortable. Vehicles will therefore be more seen as nodes of a mobile and collective network (also known as Vehicular Ad-Hoc Network, or VANET) rather than individual vehicles. Significant interest in ITS can be observed in several projects around the world: GeoNet [2], SPITS [3], CVIS [4], and RITA [5], just to name a few of them.

By enabling vehicles to communicate with each other as well as with roadside units, a new horizon of location-aware services is foreseen. Geocast is one example of a location-aware service that enables messages to be sent to a set of vehicles within specific areas defined by latitude and longitude coordinates [6]. Geocast has shown particular interest in the automotive domain [7], in which geocast messages could be sent from back offices on the Internet to specific road sections in order to warn drivers of hazards that may be lying ahead. These messages could be geocasted directly (e.g., via base stations in the vicinity) or through multiple wireless hops (e.g., car to car).

Within the context of Internet-based communications, geo-

graphical coordinates must be associated with IPv6 addresses¹ in order for geocast to properly work. This association is of greatest importance when you need to delivery information to all IPv6 nodes within a certain geographical area. However, geographical information is still somehow missing in IP addressing whereas the use of geographical addressing has already been studied on cellular networks [8] [9] [10].

Proposals to associate geographical information into the (logical) addressing mechanism used on the Internet can be found in the literature. We identify three main proposals as follows: GPS-based messaging [11], geographical IPv6 prefix format [12], and extended DNS [13]. The first solution proposes the introduction of routers that are aware of their geographical areas and exchange this information with other geographical routers. In its turn, the second solution consists in encoding geographic locations as part of the IPv6 prefix and then routing IPv6 packets appropriately. At last, the third solution proposes to extend Domain Name System (DNS) servers with a geographic information database. For that, a new top level domain should be added, namely *.geo*.

However, the aforementioned proposals present some shortcomings. The GPS-based messaging requires the deployment of a new physical structure in order to work. Next, the second solution associates ranges of IPv6 addresses with squares of different sizes representing the world surface. Other geometrical shapes besides squares are however not defined in this solution. Finally, in the extended DNS solution the addition of *.geo* as a new generic top-level domain has been proposed, but it failed to gain approval.

The motivation of our proposal comes from the fact that current proposals require either the implementation of specialized GPS-based hardware or the introduction of a new generic top-level domain. These proposals demand a considerable effort to integrate VANETs with the current infrastructure of the Internet, which make us skeptical about their acceptance. The integration of VANETs with the Internet is envisaged to enable vehicles to rely on protocols that have constantly been

¹We assume that VANETs will primarily use IPv6 addresses due to the lack of IPv4 addresses for the likely great number of VANET elements (vehicles and roadside units).

enhanced and have proved to be effective on a global scale.

Within this context, the goal of this paper is to introduce a new proposal in the scope of VANETs. Our proposal consists in providing means for back offices on the Internet to send IPv6 packets through roadside units to multiple vehicles within a designated area. This could be useful for back offices to inform drivers about, for instance, extraordinary road conditions (e.g., slippery road) or traffic conditions (e.g., traffic jams). We highlight although our proposal is not limited to a single-purpose geocasting, but it is aimed at providing general-purpose geocasting. It is also worth mentioning that we envisage no major modifications to the Internet as opposed to the aforementioned proposals.

The main challenge to be addressed in this paper is how back offices resolve IPv6 addresses of roadside units given specific geographical locations. For that, we target at extending DNS based on location (LOC) records defined in the RFC 1876 [14]. The main reason to use DNS is due to its scalable infrastructure, since the number of roadside units that back offices have to deal with can be considerably large. Moreover, back offices can decide whether the DNS resolution should be made public on the Internet or private in a local domain. Both resolutions are possible by using DNS principles.

One could argue that storing LOC records of vehicles in place of LOC records of roadside units would be more intuitive, since our main objective is primarily to inform vehicles within specific geographical locations. We counter-argue that by stating that storing geographical information about vehicles may not scale due to their great volume and constant mobility. If we would so, vehicles would have to register their new location with a DNS server whenever they would change their location. With numerous vehicles moving constantly, as in ITS context, it would be discouraging to update the location mapping for each one of them.

The remainder of this paper is structured as follows. In Section II we review the current state of the art on geocasting. Then, Section III introduces our proposal. Finally, we close this paper in Section IV, where we draw our conclusions and future work.

II. STATE OF THE ART

This section describes three proposals intended for geocasting: the GPS-based messaging proposal, the geographical IPv6 prefix format proposal, and the extended DNS proposal.

A. GPS-based messaging

The GPS-based messaging proposal has been introduced in [11]. It consists of performing geographic routing by applying hierarchical forwarding in a fixed network like the Internet. The GPS-based messaging proposal assumes that the fixed network has a cellular structure and that for each cell, there is a node that relays all messages for the nodes inside the cell.

Three components are considered for geographic routing: GeoRouters, GeoNodes and GeoHosts. GeoRouters are location-aware routers that are in charge of transmitting packets from a sender to a destination according to the geographic

destination information of the packets. They know therefore their services area and exchange this information with other GeoRouters. They are also arranged in a hierarchy with small service areas to enhance efficiency. In their turn, GeoNodes are in charge of storing incoming packets, with geographical information, during their lifetime and periodically multicasting them to their cell. Finally, a GeoHost is a daemon located on all hosts with capability to receive and send packets.

The routing process can be summarized into three main steps: 1) sending, 2) shuttling between GeoRouters, and 3) receiving. To send a packet, a GeoRouter uses the routing table information to determine where the final destinations for the message reside and which neighbor GeoRouters have to be sent a copy of the packet. First, the GeoRouter uses the information in the routing table to search for and discover where to send the packet. Then, the GeoRouter creates a list of the neighbor GeoRouters on the shortest paths to the destinations, and a copy of the message is sent to each neighbor GeoRouter on the list. These GeoRouters then deliver a packet to the responsible GeoNodes, and, finally, the GeoNodes deliver a packet to all users in the destination area.

Fig. 1. Geometric routing [11].

For example, in Figure 1, a node on the Busch Campus wants to send a message to the destination polygon in the College Ave. Campus. The message is first passed to the Busch Campus GeoRouter. By using geographical information in its routing table, the GeoRouter determines that the target area is not under its service area, but under the College Ave. GeoRouter service area. It then forwards the message to the county GeoRouter, since it is the next GeoRouter on the shortest path to the destination. Using the same algorithm, the county GeoRouter decides to forward the message to the College Ave. GeoRouter. In its turn, the College Ave. GeoRouter transmits the message to all the wireless cells intersecting the destination polygon.

The major shortcoming of this proposal is that it requires the introduction of a specialized physical infrastructure to perform addressing and routing geographically. Since no use of the current Internet infrastructure is done, it may require a significant effort to be deployed in VANETs.

B. Geographical IPv6 prefix format

In the redesign of IP, which resulted in the IPv6 [15], a major concern was the number of IP addresses that could be addressed. IPv6 has been conceived with a larger address space (128-bit address) than its predecessor, IPv4, which has only 32 bits. Another design decision was the allocation of the IP address type space for geographic addresses [16] [17]. As a result of that, subnets and hosts would have their addresses assigned based on geographic criteria. Since IPv6 addresses were designed to be sufficiently large, it is possible to encode geographical information in the address itself. IPv6 is therefore the IP version to be most likely used as a standard in VANETs.

A solution to reserve IPv6 address space for geographic addresses is the provider-independent global unicast address format [12]. This document defines a geographic global unicast address format for IPv6 address allocation. This format defines a mechanism that breaks down the geographic location of a site into prefix lengths. Routers then perform the routing according to prefix lengths, rather than by geographical coordinates. This mechanism does not require therefore routers to know about geography as the case of GeoRouters (Subsection II-A).

The format defined in [12] interleaves latitude and longitude magnitude information into a network number suited to the longest-prefix-match routing used on the Internet. Given the fact that the most bits of the 128-bits IPv6 address are reserved, all geographic data must fit into a 44-bits field. It is worth mentioning that the resulting 44-bits field provides a resolution grid of approximately 6.4 meters (equatorial) on a side. For instance, 20 bits of the IPv6 unicast address space can be used to represent a squared region of approximately 26 km^2 (at a resolution of 6.4 m square). By using bit interleaving, shorter prefixes can be used to represent large areas. As more bits are used, the accuracy increases. For example, 24 bits represent 6.5 km^2 (which could represent a city) whereas 36 bits represent 102 m^2 (which could represent a block in a city).

In conjunction with RFC 3306 [18], a specific capability for multicast groups could be defined by these unicast prefixes to target group members in a geographic region. Using such multicast feature, warning messages could be sent to elements in an area without the need to individually contact them.

The major shortcoming of this proposal is the representation of geographical areas as squares only. Without the ability to precisely discriminate geographical locations, such as geographical borders, some IPv6 nodes could be, for instance, inadvertently informed. In order for these nodes to avoid then receiving unintentional notifications, a relevance area should be specified and nodes should check if they lay inside it. One could also argue that it may still take some time for this proposal to be implemented, given the fact it has not been standardized yet.

Another related proposal that we briefly mention here is the use of IP prefixes in order to derive geographical information (e.g., country, region, city, latitude, longitude), and other information (e.g., connection speed, ISP and domain name) given an IP address. IP2Location databases from Hexasoft

[19] is one of the best-known examples. All IP2Location databases contain at least a range of IP addresses associated with a country name. It is worth mentioning that more detailed associations exist. Even though the main mapping process employed in the IP2Location is to obtain geographical information given an IP address, it is also possible to obtain (a range of) IP addresses given geographical coordinates. A major shortcoming is that the finest granularity used to define a geographical location is at the city level, being country level the thickest granularity. Moreover, individual IP addresses are not stored in the IP2Location databases, but a range of them.

C. Extended DNS

In this solution the authors sketch a proposal in the RFC 2009 [13] in order to extend DNS servers with a geographic information database. A new top level domain is added, namely *.geo*. The descending domain levels would represent states, counties, and polygons of geographic coordinates, respectively. Based on that, a geographic address could look like this: *University-of-Twente.Enschede.Overijssel.The-Netherlands.geo*. Geographic addresses are then resolved into a set of IP addresses belonging to the destination area and routing is performed accordingly.

Even though this solution is sounded, the extended DNS proposed in the RFC 2009 has been conceived as a sketch by its authors and not further discussed. In addition to that, *.geo* was proposed by Stanford Research Institute (SRI) International to the Internet Corporation for Assigned Names and Numbers (ICANN) in 2000 as a new generic top-level domain, but it failed to gain approval. Since then, there has not been any noticeable activity regarding this proposal for several years [20].

Another proposal to extend the Domain Name System with geographical capabilities is the RFC 1712 [21], which was formerly normative, but it has now been obsoleted by the RFC 1876 [14]. This latter RFC introduces the DNS LOC (location) resource record, which allows the DNS to store geographical information about hosts, networks, and subnets. By performing then forward DNS lookups, geographical information about hosts or domains can be obtained. Current implementation of DNS, such as BIND [22], support LOC records to be inserted in the master file. The LOC record has the following format:

```
<owner> <TTL> <class> LOC ( d1 [m1 [s1]]  
"N"|"S" d2 [m2 [s2]] "E"|"W" alt["m"]  
[siz["m"]] [hp["m"]] [vp["m"]]] )
```

where *d1* is the latitude in degrees from 0 to 90, *d2* is the longitude in degrees from 0 to 180, *m1* and *m2* are minutes from 0 to 59, *s1* and *s2* are seconds from 0 to 59.999, *alt* is the altitude in meters from -100000.00 to 42849672.95, and *siz*, *hp*, *vp* are, respectively, size, horizontal precision, and vertical precision expressed in meters from 0 to 90000000.00. If omitted, minutes and seconds default to zero, size defaults to 1 m, horizontal precision defaults to 10000 m, and vertical precision defaults to 10 m. It is worth of

mentioning that the parentheses are used for multi-line data as specified in RFC 1035 [23] (section 5.1).

An example of a DNS LOC resource record would be as follows:

```
example.com. IN LOC 37 23 30.900 N 121 59
19.000 W 7.00m 100.00m 100.00m 2.00m
```

This LOC record could then be looked up as follows:

```
$ host -t LOC example.com
example.com location 37 23 30.900 N 121 59
19.000 W 7.00m 100.00m 100.00m 2.00m
```

We see LOC records as the proposal requiring less effort to be put in practice. LOC records are already supported in current DNS implementations and it is only required that network administrators change DNS records in order to add geographical location for hosts and domains. It is worth highlighting that LOC records provide means to express geographical locations as different geometrical shapes, such as circles or polygons. Moreover, LOC records also provide means to express altitude, which allows to discriminate hosts located at different elevations. A minor disadvantage that we see is that the geographical information can be maliciously manipulated in the sense that there is no easy way of verifying the accuracy of the location entered [24].

III. OUR PROPOSAL

This section introduces our proposal for geocasting towards VANETs. We start with an overview about DNS and VANET. Following that, we present how geographical information of transport infrastructures can be expressed as LOC records. Finally, we present how geocasting can be achieved with our proposal.

A. A bit about DNS

DNS currently supports two kinds of lookups: forward DNS lookup and reverse DNS lookup. The former performs a lookup using an Internet hostname to find an IP address, where the latter performs a lookup using an Internet IP address to find a hostname. It is worth saying that in the forward DNS lookup, other information associated with hostnames can also be obtained, such as mail exchangers within a domain (the MX resource record).

Our proposal to extend DNS in order to support geographical queries is based on the RFC 1876 [14]. In our proposal, DNS servers are extended with the capability to resolve geographical locations into IP addresses, without requiring changes in the routing behavior of today's Internet. The key point of our proposal is the use of LOC records as primary key in the forward DNS lookup in order to return IP addresses associated with geographical locations. In other words, we basically aim at introducing a new primary key into DNS besides the already existing ones (hostnames and IP addresses). For

that, we only foresee modification in the current DNS server implementations instead of requiring specialized hardware and software or introducing new protocols. It is worth mentioning that the translation from IP address into geographical location can also be performed (See RFC 1876 [14], section 5.2.2). In this translation, an IP address is first mapped to a name using the IN-ADDR.ARPA namespace [25] and then the LOC record associated with that name is returned.

B. A bit about VANET

We identify three main VANET elements as participating in our proposal: Vehicles on-board units (OBU), Roadside units (RSU), and Back offices (BO). An OBU is a physical device located in a vehicle and responsible for Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications. It acts as a mobile router in-vehicle in charge of communicating with other vehicles, RSUs and BOs located in the Internet. In its turn, a RSU is an IPv6 router with at least one IEEE 802.11p-based egress interface and one ingress interface connecting to other IPv6 nodes. A RSU can be in charge therefore of forwarding data (acting thus as an IPv6 access router) or providing access to OBUs. Finally, a BO can communicate with RSUs or OBUs for infotainment or warning messages.

The communication involving these VANET elements can be divided into: *infrastructure-based communications* and *infrastructure-less communications*. In the former, vehicles communicate with elements fixedly located in a network infrastructure, such as RSUs and BOs. On the other hand, in the latter, the communication is among vehicles alone without infrastructure support (Figure 2). This paper considers infrastructure-based communications. The communication among vehicles (infrastructure-less communications) is out of the scope. We foresee although geocast routing protocols [7] playing a major role in V2V communications.

Fig. 2. The VANET elements.

The main focus of this paper is on IPv6 Internet-based geobroadcast. It consists in back offices located on the Internet sending IPv6 packets through roadside units to multiple vehicles within a designated area. In other words, IPv6 packets are transmitted from an Internet source to a roadside unit and

then geobroadcasted to the service area of the roadside unit. From there on, IPv6 packets may be multi-hopped between the roadside unit and the vehicles. The destination range is therefore multiple vehicles within specified geographical areas, which characterizes as geobroadcast.

We consider the GeoNet architecture [26] as reference to this paper. Our proposal can be contextualized with the module 0A: Geo-destination presented in the GeoNet architecture (Figure 3).

Fig. 3. Main functional modules of the GeoNet architecture [26].

The module 0A: Geo-destination is in charge of providing information about the geographic area where IPv6 packets shall be transmitted to. It works therefore as a cross-layer module in the management layer and it is accessed by the application and the C2CNet layers through MNG-UL and MNG-C2C SAPs, respectively. The module 0A: Geo-destination can be seen as providing means for these layers to have a common understanding about a geographical destination.

C. Extended DNS meets VANETs

In order to enable IPv6 Internet-based geobroadcast, we introduce our extended DNS proposal, which we refer to as eDNS from now on. The main idea here is that a back office queries the eDNS server with geographical coordinates and it receives RSU(s) IPv6 address(es) in return.

LOC records allow locations to be expressed as circles or polygons. Within the context of VANETs, we could have therefore geographical coordinates of a motorway stored as a polygon in the DNS master file. RSUs along the motorway could cover different road sections and the geographical coordinates of these sections would be stored in the DNS master file as polygons too. Translating this to the DNS terminology, the motorway could be seen as a domain, the motorway sections could be seen as subdomains, and the RSUs would be the hostnames within each subdomain.

Geographical information of RSUs is stored in the DNS master file based on their wireless coverage area. Since wireless coverage area can be affected by many factors, especially in urban areas [27], we deliberately simplify the wireless coverage area of a RSU as being an area of the road section assigned to the RSU. However, we are aware of the fact that measurements should be performed in order to precisely certify the coverage area of a RSU.

RSUs could have multiple wireless technologies but, for convenience, in this paper we assume only IEEE 802.11p [28] as wireless link. Given the fact that wireless communication with 802.11p can reach several hundred meters, we attribute a road section per RSU. We envisage road sections assigned to each RSUs as being adjacent and non-overlapping (Figure 4). Figure 4 depicts an ideal arrangement of RSUs along the road, but this can be unrealistic in some cases. More details about this will be addressed in Subsection III-D.

Fig. 4. Representing VANET elements as geographical coordinates.

With RSU's geographical information in the DNS master file, DNS servers would accordingly update the mapping for the RSU's IPv6 address. Taking as example the Dutch A35 motorway depicted in Figure 4 along with its RSUs, we show in Figure 5 how it could be represented in the DNS master file through the use of LOC records.

```
$TTL 24h
; Road domain
a35.highways.nl. IN SOA ns.a35.highways.nl. root.a35.highways.nl. (
    2007062800 ; serial number
    3h ; refresh time
    30m ; retry time
    7d ; expire time
    3h ; negative caching ttl
)

; Nameservers
a35.highways.nl IN NS ns.a35.highways.nl.

; A35 geographical coordinates
a35.highways.nl IN LOC (52 14 20 N 6 51 20 E) (52 14 22 N 6 51 24 E)

; RSUs
rsu1.a35.highways.nl. IN AAAA 3FFE:801:1000::2EF:6FFF:FE11:2222
rsu1.a35.highways.nl. IN LOC (52 14 20 N 6 51 20 E) (52 14 22 N 6 51 21 E)
rsu2.a35.highways.nl. IN AAAA 3FFE:801:2000:100:280:9AFF:FE80:3333
rsu2.a35.highways.nl. IN LOC (52 14 20 N 6 51 21 E) (52 14 22 N 6 51 22 E)
rsu3.a35.highways.nl. IN AAAA 3FFE:801:3000:1:270:9AFF:CH80:4444
rsu3.a35.highways.nl. IN LOC (52 14 20 N 6 51 22 E) (52 14 22 N 6 51 23 E)
rsu4.a35.highways.nl. IN AAAA 3FFE:801:4000:100:2500:8AEF:FEHH:3542
rsu4.a35.highways.nl. IN LOC (52 14 20 N 6 51 23 E) (52 14 22 N 6 51 24 E)
```

Fig. 5. Representing VANET elements in the DNS master file.

The A35 motorway could be defined as a DNS domain `a35.highways.nl`. We represent then the length of the A35 motorway as LOC records in the master file. `ns.a35.highways.nl` is the name of the eDNS server that is in charge of resolving geographical queries under its

local administrative domain (i.e., `a35.highways.nl`). The master file also includes the IPv6 addresses and LOC records of the RSUs along A35.

When performing a forward DNS lookup, the RSU name would be the primary key of a query issued to `ns.a35.highways.nl`. Thus, querying `rsu1.a35.highways.nl` would result in a lookup where all fields associated with RSU1 (IPv6 address and location) are returned. In our eDNS proposal, we use instead the LOC record as the primary query and the associated information (hostname and IPv6 address) with the LOC record is returned. Such query could look something like this:

```

; Request
QNAME = "(52 14 20 N 6 51 22 E) (52 14 22 N 6 51 23 E).a35.highways.nl"
QTYPE = Host Address
;
; Answer
NAME = "(52 14 20 N 6 51 22 E) (52 14 22 N 6 51 23 E).a35.highways.nl"
TYPE = Host Address
RDATA = Type AAAA, addr 3FFE:801:3000:1:270:9AFF:CH80:4444

```

Fig. 6. Example of a geobroadcast query to an eDNS server.

As depicted in Figure 6, a DNS request with the geographical coordinates of the road section 3 is issued, and as a result the IPv6 address of RSU3 is returned. It is worth highlighting that the DNS request depicted in Figure 6 is just a sketch. When more details on the hierarchy of eDNS servers become clearer for us, the way this request is issued may be changed.

The eDNS is envisaged to calculate the intersection between the issued geographical coordinates and the LOC records through strategies used in computational geometry [29]. Point in polygon algorithms [30] could, for example, be used to test whether a set of points representing geometric shapes (e.g., squares or circles) lie inside or outside of a polygon. Within the context of VANETs, such strategies would verify therefore whether a RSU covers the whole area of an issued geobroadcast or at least part of it.

The performance of best-known point in polygon algorithms is practically linear given the number of edges per polygon [30]. Equally relevant, these algorithms can be considered relatively fast (some few microseconds) when the number of edges per polygon is few in amount (i.e., less than 10 edges). We aim at testing some point in polygon algorithms within the context of DNS, in which DNS servers are expected to get a large amount of queries per second.

D. Geobroadcasting with eDNS

Geobroadcasting with eDNS consists in a back office being first notified (either by sensors along the road or vehicles passing by) about an abnormal road condition that needs attention by drivers, and then issuing a warning message to a specified geocast region. Figure 7 shows an example scenario in which a vehicle detects black ice on the road. It then broadcasts this information to its vicinity. RSU1 receives the traffic hazard message and it sends this information to a traffic back office server located on the Internet. Based on the received information, the back office server decides to send

a warning message to a specified geocast region. It then first queries the eDNS server with the geographical coordinates of the geocast region. The eDNS server performs a lookup in its database and it finds out that the geocast region is within the RSU3's road section. The eDNS server then returns the RSU3's IPv6 address to the back office server. Finally, the back office server contacts RSU3 in order to request it to broadcast a warning message ("Icy road" in our example) to all vehicles in the specific geocast region.

Fig. 7. Example of a back office server interacting with an eDNS server.

It is worth saying that the example depicted in Figure 7 shows a scenario in which there are no gaps among RSUs. However, this may not be realistic in all cases, specially in rural areas, where there is very little or no fixed communication infrastructure available [31]. In such areas, it may happen that no intersection between the geocast region and any covered road section occurs.

One possibility to overcome this issue would be to send the geocast message to the RSU closest to the geocast region or even to multiple RSUs in the vicinity of the geocast region. Then multi-hop communication is used to reach vehicles in the geocast region. In order to enhance the probability of delivery, we also consider to choose RSUs that are close to the geocast region and that have a high density of vehicles transiting in their road sections. With more vehicles receiving the geocast message, there is a higher probability that these vehicles deliver the geocast message via multi-hop to the geocast region.

In ITS context, vehicles are expected to periodically transmit short status messages (beacons). They contain information, such as speed and position, from which a cooperative awareness can be established [32]. A RSU could then calculate how dense its road section is based on the amount of beacons received from vehicles transiting the road section. RSUs could then report their density to the eDNS server that, in its turn, would decide to which RSU the message should be sent by using dynamic load balancing techniques [33].

IV. CONCLUSIONS AND FUTURE WORK

This paper presents a description of our proposal to extend DNS in order to support geographical capabilities. Our main contribution is that our proposal is foreseen to require only few modifications in existing DNS implementations. Moreover, our proposal does not require the introduction of any specialized hardware or software, neither the modification of any existing protocol. In other words, we aim at extending DNS with what it is available out there.

We believe that the use of DNS principles, more specifically the distributed DNS hierarchy, may play a major role when scalability is an issue. Taking into account, for instance, that the number of RSUs along highways is expected to be large (in order to provide optimum wireless coverage), keeping records of such RSUs in a centralized way may become a bottleneck. Moreover, if confidentiality is desired, the hierarchy of DNS servers can be privately employed in a local domain. That would avoid sensitive information about RSUs to be disclosed.

We already foresee although a couple of challenges ahead. To name a few of them, the hierarchy of eDNS servers in our proposal is still an open issue, since the combination of logical domain names may not reflect the geographical location of such domains. For instance, different levels of hierarchy could be needed in order to make our proposal scalable. Another challenge is with regard to the performance of computational geometry algorithms. With a large amount of polygons (representing geographical areas), the running time of such algorithms can become a bottleneck.

As future research, we aim at performing an implementation and validation of our proposal. Our idea is to extend DNS by modifying a DNS implementation (e.g., BIND), and then testing it in a small scale domain (e.g., a single administrative domain), but with extension plans to larger domains.

Acknowledgments: This research work has been supported by the Dutch *HighTech Topproject* HTT09005, viz., Strategic Platform for Intelligent Traffic Systems (SPITS). The authors would like to thank Martijn van Eenennaam, Wouter Klein Wolterink, and Georgios Karagiannis for their valuable comments on this topic.

REFERENCES

- [1] Wikipedia, "Intelligent transportation system," September 2010. [Online]. Available: http://en.wikipedia.org/wiki/Intelligent_transportation_system
- [2] GeoNet, "GeoNet project," September 2010. [Online]. Available: <http://www.geonet-project.eu/>
- [3] SPITS, "SPITS," September 2010. [Online]. Available: <https://spits-project.com/>
- [4] CVIS, "CVIS," September 2010. [Online]. Available: <http://www.cvisproject.org/>
- [5] RITA, "RITA," September 2010. [Online]. Available: <http://www.its.dot.gov/index.htm>
- [6] J. C. Navas and T. Imielinski, "GeoCast—geographic addressing and routing," in *MobiCom '97: Proceedings of the 3rd annual ACM/IEEE international conference on Mobile computing and networking*. New York, NY, USA: ACM, 1997, pp. 66–76.
- [7] C. Maihofer, "A survey of geocast routing protocols," *IEEE Communications Surveys Tutorials*, vol. 6, no. 2, pp. 32–42, 2004.
- [8] Y. Zhao, "Standardization of mobile phone positioning for 3G systems," *IEEE Communications Magazine*, vol. 40, no. 7, pp. 108–116, July 2002.
- [9] K. Kyamakya and K. Jobmann, "Location management in cellular networks: classification of the most important paradigms, realistic Simulation framework, and relative performance analysis," *IEEE Transactions on Vehicular Technology*, vol. 54, no. 2, pp. 687–708, March 2005.
- [10] M. Balakrishnan, I. Mohamed, and V. Ramasubramanian, "Where's that phone?: geolocating IP addresses on 3G networks," in *IMC '09: Proceedings of the 9th ACM SIGCOMM conference on Internet measurement conference*. New York, NY, USA: ACM, 2009, pp. 294–300.
- [11] T. Imieliński and J. C. Navas, "GPS-based geographic addressing, routing, and resource discovery," *Communications of the ACM*, vol. 42, no. 4, pp. 86–92, April 1999.
- [12] T. Hain, "An IPv6 Geographic Global Unicast Address Format," Internet Draft draft-hain-ipv6-geo-addr-02.txt, Internet Engineering Task Force, 2010.
- [13] T. Imielinski and J. Navas, "GPS-Based Addressing and Routing," RFC 2009 (Experimental), Internet Engineering Task Force, Nov. 1996.
- [14] C. Davis, P. Vixie, T. Goodwin, and I. Dickinson, "A Means for Expressing Location Information in the Domain Name System," RFC 1876 (Experimental), Internet Engineering Task Force, Jan. 1996. [Online]. Available: <http://www.ietf.org/rfc/rfc1876.txt>
- [15] S. Deering and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification," RFC 2460 (Draft Standard), Internet Engineering Task Force, Dec. 1998. [Online]. Available: <http://www.ietf.org/rfc/rfc2460.txt>
- [16] Y. Rekhter and T. Li, "An Architecture for IPv6 Unicast Address Allocation," RFC 1887 (Informational), Internet Engineering Task Force, Dec. 1995. [Online]. Available: <http://www.ietf.org/rfc/rfc1887.txt>
- [17] R. Hinden and S. Deering, "IP Version 6 Addressing Architecture," RFC 2373 (Proposed Standard), Internet Engineering Task Force, Jul. 1998. [Online]. Available: <http://www.ietf.org/rfc/rfc2373.txt>
- [18] B. Haberman and D. Thaler, "Unicast-Prefix-based IPv6 Multicast Addresses," RFC 3306 (Proposed Standard), Internet Engineering Task Force, Aug. 2002. [Online]. Available: <http://www.ietf.org/rfc/rfc3306.txt>
- [19] Hexasoftware, "IP2Location," September 2010. [Online]. Available: <http://www.ip2location.com/>
- [20] Wikipedia, "geo," September 2010. [Online]. Available: <http://en.wikipedia.org/wiki/geo>
- [21] C. Farrell, M. Schulze, S. Pleitner, and D. Baldoni, "DNS Encoding of Geographical Location," RFC 1712 (Experimental), Internet Engineering Task Force, Nov. 1994. [Online]. Available: <http://www.ietf.org/rfc/rfc1712.txt>
- [22] ISC, "BIND — Internet Systems Consortium," September 2010. [Online]. Available: <http://www.isc.org/software/bind>
- [23] P. Mockapetris, "Domain names - implementation and specification," RFC 1035 (Standard), Internet Engineering Task Force, Nov. 1987. [Online]. Available: <http://www.ietf.org/rfc/rfc1035.txt>
- [24] V. N. Padmanabhan and L. Subramanian, "An investigation of geographic mapping techniques for internet hosts," *ACM SIGCOMM Computer Communication Review*, vol. 31, no. 4, pp. 173–185, October 2001.
- [25] P. Mockapetris, "Domain names - concepts and facilities," RFC 1034 (Standard), Internet Engineering Task Force, Nov. 1987. [Online]. Available: <http://www.ietf.org/rfc/rfc1034.txt>
- [26] GeoNet, "D1.2 Final GeoNet Architecture Design," <http://www.geonet-project.eu/?download=GeoNet-D.1.2-v1.2.pdf>, June 2010.
- [27] S. Sai, E. Niwa, K. Mase, M. Nishibori, J. Inoue, M. Obuchi, T. Harada, H. Ito, K. Mizutani, and M. Kizu, "Field evaluation of UHF radio propagation for an ITS safety system in an urban environment," *IEEE Communications Magazine*, vol. 47, pp. 120–127, November 2009.
- [28] Wikipedia, "IEEE 802.11p," September 2010. [Online]. Available: http://en.wikipedia.org/wiki/IEEE_802.11p
- [29] —, "Computational geometry," September 2010. [Online]. Available: http://en.wikipedia.org/wiki/Computational_geometry
- [30] E. Haines, *Point in polygon strategies*. San Diego, CA, USA: Academic Press Professional, Inc., 1994, pp. 24–46.
- [31] M. Zhang and R. Wolff, "Routing protocols for vehicular Ad Hoc networks in rural areas," *IEEE Communications Magazine*, vol. 46, no. 11, pp. 126–131, November 2008.
- [32] E. M. van Eenennaam, G. Karagiannis, and G. J. Heijnen, "Towards Scalable Beaconing in VANETs," in *Fourth ERCIM workshop on eMobility, Luleå, Sweden*. Luleå, Sweden: Luleå University of Technology, Luleå, Sweden, May 2010, pp. 103–108.
- [33] V. C. Harish and B. Owens, "Dynamic Load Balancing DNS," *Linux Journal*, p. 11, August 1999.