

Extending the Domain Name System (DNS) to Provide Geographical Addressing towards Vehicular Ad-Hoc Networks (VANETs)

Tiago Fioreze and Geert Heijenk

University of Twente
Centre for Telematics and Information Technology (CTIT)
Department of Design and Analysis of Communication Systems (DACS)
Enschede, The Netherlands
{t.fioreze,geert.heijenk}@utwente.nl

Abstract—Geographical addressing is a key communication paradigm in emerging Intelligent Transportation Systems (ITS). In this paper, we address the issue of how to direct messages to roadside units (RSUs) in order to have them forwarded by the RSUs to the on-board units (OBUs) of vehicles in a certain specified destination area. For that purpose, we have extended the Domain Name System (DNS) to support geographically scoped queries. A query with specified geographical coordinates will be resolved by the extended DNS system to the IPv6 addresses of those RSUs that cover the area described by the geographical coordinates. In this paper, we further extend the proposal by introducing delegation of geographical queries to DNS servers lower in the hierarchy. Furthermore, we demonstrate the feasibility of the proposal by implementing and experimenting with a prototype.

I. INTRODUCTION

Governments worldwide and mobility industry are encouraging research and innovation on Intelligent Transportation Systems (ITS). ITS envisage information to be shared among vehicles, and between vehicles and roadside units through wireless communications technology in order to improve safety, avoid congestion, provide services to drivers, and reduce the environmental impact of mobility. Significant interest in ITS can be observed in several projects around the world: GeoNet [1], SPITS [2], CVIS [3], and RITA [4], just to name a few of them.

ITS can vary in the way technologies are applied. They can be applied from basic car navigation systems to more advanced technologies, such as lane merging assistants. This paper focuses on the use of geocast technologies to deliver information to destinations specified by geographical constraints [5].

Within the ITS context, 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. Geocast has shown particular interest in the automotive domain [6] [7], in which geocast messages could be sent from back offices on the Internet to specific road sections in order to warn drivers of road hazards. These messages could be geocasted directly (e.g., via nearby base

stations) or through multiple wireless hops (e.g., car to car).

There is a strong tendency in the automotive research community to integrate ITS with the current infrastructure of the Internet. This integration is envisaged to enable vehicles to rely on protocols that have constantly been enhanced and have proved to be effective on a global scale. In order for geocast to properly work in the context of Internet-based communications, geographical coordinates must be associated with IPv6 addresses¹. This association is of greatest importance when information needs to be delivered to all IPv6 nodes within a certain geographical area.

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

To achieve that, we have proposed in a previous work of ours [8] the extension of the Internet Domain Name System, so that queries based on location can be carried out. Upon receiving such a query, this scalable, global system will return the IPv6 addresses of RSUs that can be used to distribute warning messages within specific geographical locations. Our proposal, eDNS, has been based on location (LOC) records defined in the RFC 1876 [9]. The use of DNS is due to its scalable infrastructure, since the number of roadside units dealt with by back offices can be significantly large.

It is also important here to highlight that even though our primary objective is to inform vehicles within specific geographical locations, we do not store location records of vehicles. That is due to the fact it may not scale well because

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).

of their great volume and constant mobility. 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.

In this paper, we extend our previous work and validate it by presenting a prototype based on NSD [10], which is an open-source server program for the DNS developed by NLnet Labs of Amsterdam in cooperation with the RIPE NCC. The main contributions of this paper are therefore (1) the extension of eDNS with capabilities to delegate queries to eDNS servers lower in the hierarchy, and (2) the evaluation of the proposed extended DNS system by means of a prototype that is capable of resolving geographical queries into IPv6 addresses.

The remainder of this paper is structured as follows. In Section II we review the current state of the art on geonetworking. Then, Section III explains how we extended a DNS implementation. In Section IV we give some thoughts on how we perform DNS delegation within the context of vehicular networks. Following that, Section V shows our prototype. Finally, we close this paper in Section VI, where we draw our conclusions and future work.

II. STATE OF THE ART

This section describes three proposals intended for geocasting: the GPS-based addressing and routing proposal, the GeoNet project, and our previous work.

A. GPS-based addressing and routing

The GPS-based addressing and routing proposal has been discussed by Imieliński [11] [12]. Imieliński proposed a general concept of sending a message to all recipients within a geographical area. A destination geographical area would be represented by some closed polygon (e.g., a circle), which would then be translated into geographic coordinates in order for messages to be sent to clients located within the bounds of that polygon. In order to do that geographic routing would be performed 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.

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. GeoNet project

The European FP7 project GeoNet [13] [14] has developed an architecture and protocol stack for geographical networking (Figure 1). Two main protocol layers have been defined. The first one is the C2CNet layer, which extends link layers such as IEEE 802.11p or ETSI ITS G5 to a sub-IP layer, providing wireless multi-hop communications with position-based forwarding. It provides among others geounicast, geobroadcast, geoanycast, topological broadcast, and store-carry-forward services within a local network. For knowledge about locations of neighboring nodes in the subnetwork, C2CNet relies on periodic beaconing. In order to obtain locations of other nodes in the network, a location service is provided.

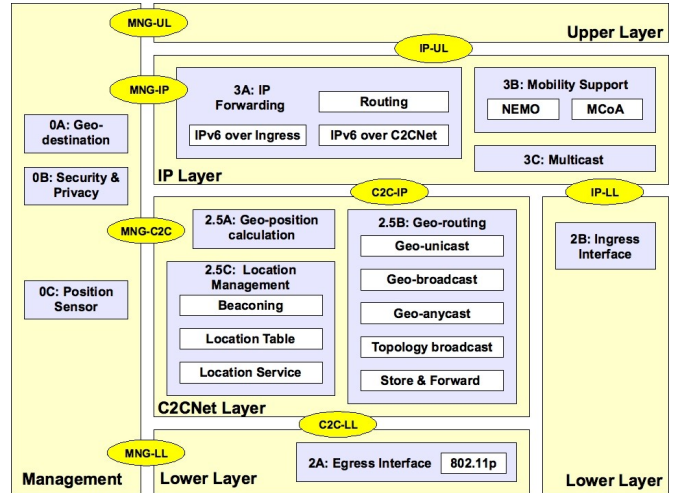


Fig. 1. Main functional modules of the GeoNet architecture [13].

The second layer, the GeoNet project was focussing on, is the IP layer. Adaptation to the IP layer have been made to make it run over C2CNet as a sub-IP layer. In order to provide geobroadcasting services in IPv6, multicast is used. In order for nodes to receive geobroadcast messages for a certain area, they have to join a predefined multicast group. Other nodes

wishing to geobroadcast to that (predefined) area send packets to such a multicast address.

Whereas the use of multicast to provide geobroadcast services aligns very well with the current Internet architecture, some serious problems remain open. If geobroadcasting is to be deployed on an Internet-wide scale, serious scalability problems may arise. Furthermore, in this approach, geocast areas have to be predefined, and cannot be chosen by the user of the service. It is worth mentioning that we are currently working on an approach to integrate the work presented in this paper with the proposals from the GeoNet project.

C. Our extended DNS (eDNS) proposal

In our previous work [8], we proposed to extend DNS implementations rather than modifying the DNS protocol, requiring new top level domains or requiring changes in the routing behavior of today's Internet. Our proposal is based on DNS LOC (location) resource records defined in the RFC 1876. Through the use of LOC records, geographical information about hosts, networks, and subnets can be stored in the DNS files. By performing then forward DNS lookups, geographical information about hosts or domains can be obtained. Current implementation of DNS, such as NSD, 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 [15] (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
```

The key point of our proposal has been 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 introduce a new primary key into DNS besides the already existing ones (hostnames and IP addresses). For that, we have suggested the modification of a DNS implementation 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 [9], section 5.2.2). In this translation, an IP address is first mapped to a name using the IN-ADDR.ARPA namespace [16] and then the LOC record associated with that name is returned.

III. OUR EDNS EXTENSION

To validate our proposal introduced in [8], we have developed a prototype, which is described in this section.

A. Communication scenario

We identify three main VANET elements as participating in our prototype: 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 an in-vehicle mobile router in charge of communicating with other vehicles, RSUs, and BOs located on 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 or providing access to OBUs. Finally, a BO can communicate with RSUs or OBUs for infotainment, traffic efficiency, and/or warning messages.

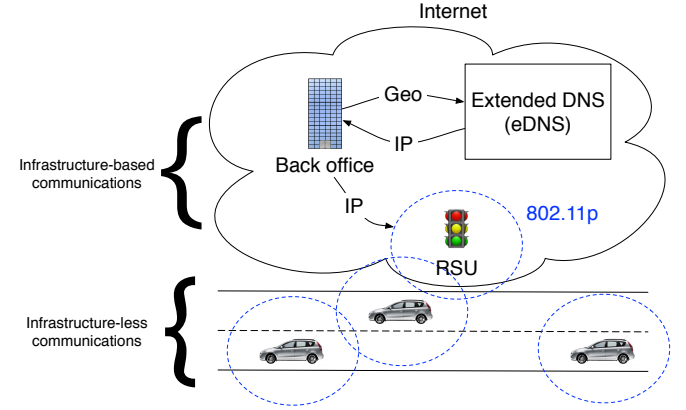


Fig. 2. The VANET elements.

The communication involving these VANET elements can be divided into: *infrastructure-based communications* and *infrastructure-less communications* (Figure 2). In the former, vehicles communicate with elements (e.g., RSUs and BOs) fixedly located in a network infrastructure. Whereas, in the latter, the communication is among vehicles alone without infrastructure support. This paper considers infrastructure-based communications. The communication among vehicles is out of the scope, but we believe geocast routing protocols [6] may play a major role for that.

B. Geobroadcasting with eDNS

In order to enable IPv6 Internet-based geobroadcast, our extended DNS prototype gives to back offices located on the Internet the means to issue our eDNS prototype with geographical coordinates and receive RSU(s) IPv6 address(es) in return. The back office is first notified (either by sensors along the road or vehicles passing by) about an abnormal road condition that needs attention by drivers, and it then issues a warning message to a specified geocast region.

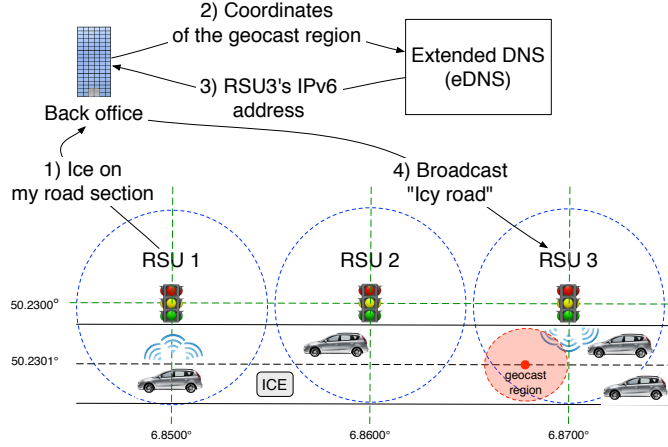


Fig. 3. Example of a back office server interacting with an eDNS server.

Figure 3 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 coverage area. 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.

C. RSU - OBU communication

Geographical information of RSUs is stored in the DNS master file based on their wireless coverage area. Wireless coverage area can however be affected by many factors, especially in urban areas [17]. For ease of explanation, we simplify the wireless coverage area of a RSU as being circular (even though LOC records allow other shapes to be expressed, such as polygons). RSUs could have multiple wireless technologies but, for convenience, we assume only IEEE 802.11p [18]. Since wireless communication with 802.11p can reach several hundred meters, we attribute a road section per RSU.

Figure 4 depicts an ideal arrangement (i.e., with no gaps) among the RSUs along the road. However, this may not be realistic in all cases, specially in rural areas, where there is

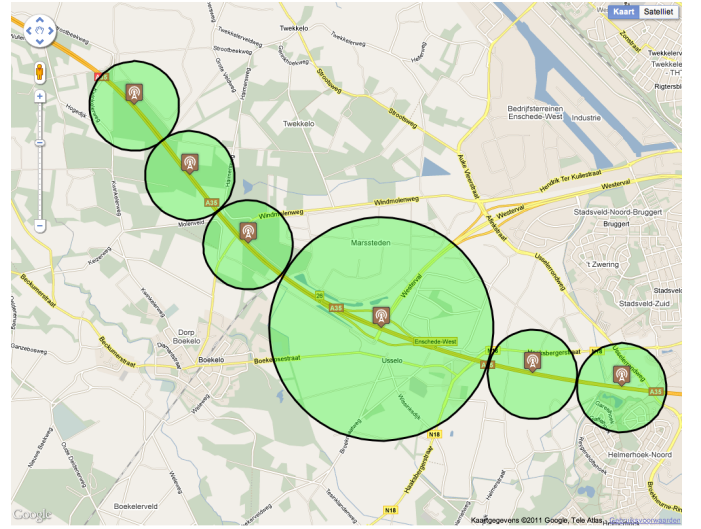


Fig. 4. An example of an ideal arrangement of RSUs along a motorway.

very little or no fixed communication infrastructure available [19]. 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 nearby 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 [20]. 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 [21].

We are also aware of the fact that measurements should be performed to precisely certify the coverage area of a RSU. A plausible solution would be to infer the coverage area based on beacons received by vehicles. If a RSU antenna receives the beacons (which contain vehicles' position), it means that the vehicle is within range and based on a set of vehicles' position a more accurate RSU coverage area can be represented.

D. Storing geographical information on RSUs into DNS

With RSU's geographical information in the DNS master file, DNS servers would accordingly update the mapping for the RSU's IPv6 address. Figure 5 shows how RSUs are represented in the DNS master file of our prototype through the use of LOC records.


```

$ORIGIN highways.nl.
$TTL      86400

; Road domain
@ IN SOA ns1.highways.nl. web-admin.highways.nl (
    2011032800 ; serial number
    3h         ; refresh time
    30m        ; retry time
    7d         ; expire time
    3h         ; negative caching ttl
)

; Nameservers
NS ns1.highways.nl.

; RSUs
rsuA1_1 IN AAAA fdda:5cc1:23:4::a11
          LOC 52 16 35.88 N 6 50 11.57 E 11m 1000m
rsuA1_2 IN AAAA fdda:5cc1:23:4::a12
          LOC 52 17 41.27 N 6 53 13.34 E 11m 1000m
rsuA1_3 IN AAAA fdda:5cc1:23:4::a13
          LOC 52 17 16.39 N 6 55 46.52 E 11m 1000m
rsuA1_4 IN AAAA fdda:5cc1:23:4::a14
          LOC 52 17 30.48 N 6 54 29.31 E 11m 400m
rsuA1_5 IN AAAA fdda:5cc1:23:4::a15
          LOC 52 17 15.39 N 6 51 50.55 E 11m 400m
rsuA1_6 IN AAAA fdda:5cc1:23:4::a16
          LOC 52 16 58.50 N 6 51 19.58 E 11m 600m
rsuA35_1 IN AAAA 3FFE:801:1000::2EF:6FFF:FE11:1111
          LOC 52 13 04.71 N 6 48 00.57 E 7m 400m
rsuA35_2 IN AAAA 3FFE:801:2000:100:280:9AFF:FE80:2222
          LOC 52 13 19.20 N 6 47 41.64 E 102m 400m
rsuA35_3 IN AAAA 3FFE:810:3000::4EF:7DDD:EF21:3333
          LOC 52 12 49.49 N 6 48 21.89 E 10m 400m
rsuA35_4 IN AAAA fdda:5cc1:23:4::1f
          LOC 52 12 25.12 N 6 49 24.79 E 11m 1000m
rsuA35_5 IN AAAA fdda:5cc1:23:4::2f
          LOC 52 12 11.35 N 6 50 38.56 E 11m 400m
rsuA35_6 IN AAAA fdda:5cc1:23:4::3f
          LOC 52 12 08.12 N 6 51 18.10 E 11m 400m
rsuA35_7 IN AAAA fdda:5cc1:23:4::4f
          LOC 52 12 01.88 N 6 53 13.88 E 11m 1000m

```

Fig. 5. Representing RSUs in the DNS master file.

The following information about a RSU is provided: name, IPv6 address, geographical location, and coverage area. For example, `rsuA1_1` is the RSU name, `fdda:5cc1:23:4::a11` is its IPv6 address, and `LOC 52 16 35.88 N 6 50 11.57 E 11m 1000m` represents its geographical location and coverage area (1000m). This latter is specified by means of a radius value (r). The area could therefore be calculated by using the formula $\pi \cdot r^2$.

```

; Request
QNAME = "(52 13 19 N 6 47 42 E 102m 100m).highways.nl"
QTYPE = Host Address
;
; Answer
NAME = "(52 13 19 N 6 47 42 E 102m 100m).highways.nl"
TYPE = Host Address
RDATA = Type AAAA, addr 3FFE801:2000:100:280:9AFF:FE80:2222

```

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

When performing a forward DNS lookup, the RSU name would be the primary key of a query issued to `ns1.highways.nl`. Thus, querying `rsuA1_1.highways.nl` would result in a lookup where all fields associated with `rsuA1_1` (IPv6 address and location) are returned. Our prototype extends the lookup

capability of DNS by enabling the use of LOC record as the primary key as well. Associated information (hostname and IPv6 address) with the LOC record can then be returned. As depicted in Figure 6, a DNS request with the geographical coordinates of the `rsuA35_2` is issued, and, as a result, the IPv6 address of `rsuA35_2` is returned.

It is worth mentioning that other elements besides RSUs can be defined in the DNS master file. For example, the LOC records of IP-based surveillance cameras could be defined here and then our proposal could be used to get the cameras that are located within a certain geographical location.

E. Calculating intersections

Our eDNS prototype calculates intersections between a geocast region and RSUs by performing the following steps:

- 1) calculate the great-circle distance between the center of the geocast region and the geographical coordinates of the RSUs. Distance (d) is calculated by using the Haversine formula [22]:

$$a = \sin^2(\Delta\text{lat}/2) + \cos(\text{lat}_1) \cdot \cos(\text{lat}_2) \cdot \sin^2(\Delta\text{long}/2)$$

$$c = 2 \cdot \text{atan2}(\sqrt{a}, \sqrt{1-a})$$

$$d = R \cdot c$$

where R is earth's radius (mean radius = 6,371km).

- 2) check if the distance (d) is smaller than the absolute value between the radius of the geocast region (r_{geo}) and the radius of each RSU (r_{rsu}), $d < |r_{geo} + r_{rsu}|$. If so, there is an intersection.

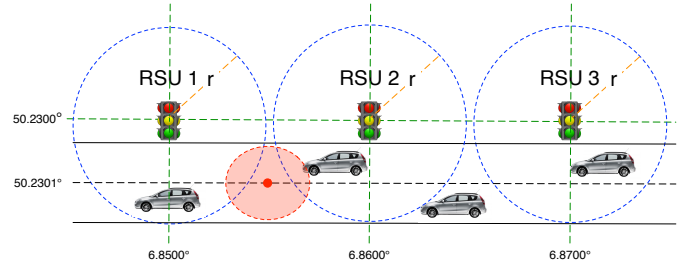


Fig. 7. Intersection between a geocast region and RSUs coverage areas.

Figure 7 shows an example where three RSUs (all with a radius of 500m) are placed along a highway and a geocast region is issued with geographic latitude of 50.2301° and geographic longitude of 6.8550° , and with a radius of 250m.

In order to calculate then if there is any intersection, our prototype first calculates the distances between the center of the geocast region and the RSUs. This would result in 356m between the geocast region and RSU1 and RSU2, and 1,067m to the RSU3. We then verify if $d < |r_{geo} + r_{rsu}|$ is true, which would mean an intersection. This would result true in the case of RSUs 1 and 2 since $356m < 750m = |250 + 500|$ and false for the RSU3 since $1067m > 750m = |250 + 500|$.

IV. eDNS DELEGATION

To make our proposal scalable a hierarchy of eDNS servers is envisaged. One could suggest the addition of a geographic information database to the DNS hierarchy, resulting in a new top level domain, namely *.geo*. The descending domain levels could 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, it was proposed in 2000 by Stanford Research Institute (SRI) International to the Internet Corporation for Assigned Names and Numbers (ICANN), but it failed to gain approval [23]. Since then, there has not been any noticeable activity regarding this proposal².

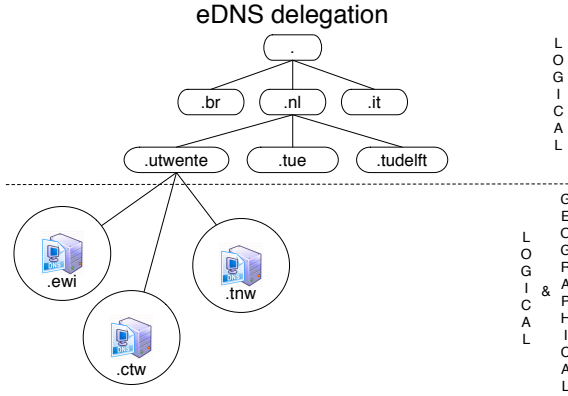


Fig. 8. Our hybrid solution.

Due to that, we believe a hybrid solution would be a more suitable solution (Figure 8). With a hybrid solution we mean that the current logical domain names could be mixed with geographical location of such domains. Moreover, this hybrid solution should work from bottom level domains to the top ones. As a result, organizations could locally implement geographical addressing without requiring top level domains to do so. Hosts could still be addressed by using a fully qualified domain name (e.g., *ewi489.ewi.utwente.nl*), but also by using the geographical query format (e.g., “(52 14 21 N 6 51 23 E 31m 5m)”.*utwente.nl*). Note that when multiple providers are covering the same area, the issuer of the geocast can select the provider of choice by specifying the last part of the domain name accordingly (here *.utwente.nl*).

Within the context of VANETs, we have created a scenario with a fictional domain: *highways.nl*, involving two eDNS servers. One of the servers is at the domain *highways.nl* and the other one is at the sub-domain *a1.highways.nl*. It is worth mentioning that our scenario fully delegates the responsibility for a sub-domain to another eDNS server. The DNS master files of these servers are shown in Figure 9.

²It is worth mentioning although that, by the time of writing this paper, ICANN has approved a plan to increase the number of generic top-level domains [24].

Fig. 9. DNS master files.

The delegation works as follows: when the eDNS server *ns1.highways.nl* receives a geographical query from a DNS client, it performs a recursive name resolution. In doing so, it responds to the client with either the requested resource record or an error message. For example, if the geographical query “(52 17 16 N 6 51 51 E 11m 100m)”.*highways.nl* is issued to *ns1.highways.nl*, it first checks whether it is authoritative for that request. If not, it then checks in its records whether there is any referral to another server. That is the case in our example, since the coverage area of the eDNS server *ns3.a1.highways.nl* intersects the issued geographical query. As a result of that, *ns1.highways.nl* fully delegates the issued geographical query to *ns3.a1.highways.nl*. Then, *ns3.a1.highways.nl* checks whether it is authoritative for the delegated request, which is the case since the geographical query intersects the coverage areas of RSU5. Finally, *ns3.a1.highways.nl* returns the answer (RSU5 resource records) to *ns1.highways.nl*, which, in its turn, returns the answer to the DNS client.

V. eDNS PROTOTYPE EVALUATION

This section presents some screenshots of our eDNS prototype in action.

Fig. 10. Example of a geographical query using command line interface.

The DNS client does not require any modification. The geographical query should follow the LOC record format defined in the RFC 1876 [9] and should be enclosed by “()”. For example, Figure 10 shows a geographical query issued to an extended DNS server hosted locally in order to request IPv6 addresses within a certain geographical location.

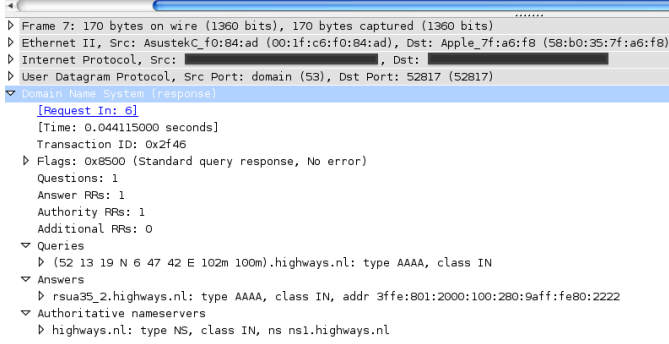


Fig. 11. Wireshark snapshot showing the answer of our eDNS server.

Figure 11 shows the DNS answer as captured from the wire through Wireshark [25]. It is worth highlighting that no error is introduced by intermediate legacy name servers when forwarding a geographical query. Sensitive information (i.e., IP addresses) in Figure 11 have been deliberately omitted.



Fig. 12. The geographical locations of RSUs and their respective coverage areas are shown here as stored in the eDNS master file.

In order to show the real potential of our extended DNS server prototype, we have used Google Maps API to graphically display the interaction between it and a normal DNS client. Figure 12 refers to the eDNS server and it shows the RSUs that are defined in the DNS master file (see Figure 5). Besides the geographical locations of the RSUs, their wireless coverage areas are also displayed.

In its turn, the DNS client is displayed in Figure 13. The DNS client is embedded in the Google Maps API and its query



Fig. 13. Performing a geographical query through drag and drop feature of Google Maps API.

is defined by using Google Maps feature of dragging a marker and dropping it. When the marker is dropped, the geographical query is triggered. The geographical query within the ITS context can be understood as a geocast region. The geocast region is defined as a circle with center point (specified by a latitude and longitude pair) and radius. Radius is defined in meters and it is adjustable. Therefore, a bigger or smaller geocast region (geographical query) can be defined.

Figure 14 shows the activity in the eDNS server. Here it is possible to see a geographical query (geocast region) that was issued to the eDNS server. It also shows that the geocast region is intersected by three RSUs served under its authority. The intersection is calculated as described in Subsection III-E.

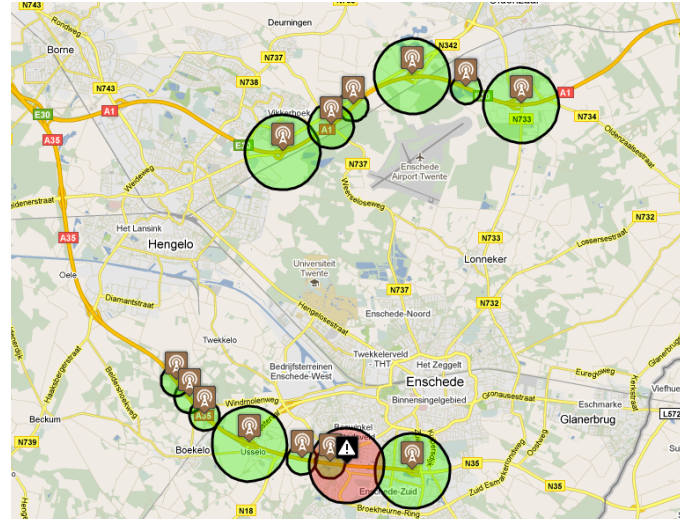


Fig. 14. The activity in the eDNS server.

Figure 15 shows the activity in the DNS client side. Here the client receives the answer from the eDNS server containing the

IPv6 addresses and LOC records of three RSUs that intersect the issued geocast region.



Fig. 15. The answer is returned to the DNS client.

VI. CONCLUSIONS AND FUTURE WORK

This paper introduces our prototype to provide geographical addressing towards VANETs. We have done that by extending a DNS implementation, NSD developed by NLnet Labs of Amsterdam in cooperation with the RIPE NCC. It is worth mentioning that even though we have used our prototype in the context of VANETs, it has been developed for a general-purpose use. Moreover, our prototype does not require the introduction of any specialized hardware or software, neither the modification of any existing protocol.

We also presented a solution to provide geographical hierarchy of eDNS servers. Our solution is both hybrid and bottom-up. Hybrid means that it mixes logical domains with the geographical information of such domains and bottom-up means that geographical domains can be specified in the lowest domains of the current DNS hierarchy. This results in no disruption of the current DNS delegation approach.

As future research, it would be interesting to provide the capability of dealing with overlapping geographical domains to our eDNS prototype. Moreover, CPU and network performances should be evaluated to show the responsiveness of our prototype. Within the context of VANETs, It would be interesting to allow the definition of different geometrical shapes in order to better reflect the wireless coverage area of RSUs. Finally, the integration of the current proposal with RSU to OBU communications for fully end-to-end geocasting is subject of further research.

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 SPITS partners as well as Martijn van Eenennaam, Wouter Klein Wolterink, and Georgios Karagiannis for their valuable comments on this topic.

REFERENCES

- [1] GeoNet, "GeoNet project," September 2011. [Online]. Available: <http://www.geonet-project.eu/>
- [2] SPITS, "SPITS," September 2011. [Online]. Available: <https://spits-project.com/>
- [3] CVIS, "CVIS," September 2011. [Online]. Available: <http://www.cvisproject.org/>
- [4] RITA, "RITA," September 2011. [Online]. Available: <http://www.its.dot.gov/index.htm>
- [5] J. C. Navas and T. Imieliński, "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.
- [6] C. Maihofer, "A survey of geocast routing protocols," *IEEE Communications Surveys Tutorials*, vol. 6, no. 2, pp. 32–42, 2004.
- [7] A. Festag, P. Papadimitratos, and T. Tielert, "Design and Performance of Secure Geo-cast for Vehicular Communication," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 5, pp. 2456–2471, June 2010.
- [8] T. Fioreze and G. Heijenk, "Extending DNS to support geocasting towards VANETs: A proposal," in *Proceedings of the Second IEEE Vehicular Networking Conference (VNC 2010)*. IEEE Communications Society, December 2010, pp. 271–277.
- [9] 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>
- [10] NLnet Labs, "NSD — NLnet Labs," September 2011. [Online]. Available: <http://www.nlnetlabs.nl/projects/nsd/>
- [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. Imieliński and J. Navas, "GPS-Based Addressing and Routing," RFC 2009 (Experimental), Internet Engineering Task Force, Nov. 1996.
- [13] GeoNet, "D1.2 Final GeoNet Architecture Design," <http://www.geonet-project.eu/?download=GeoNet-D.1.2-v1.2.pdf>, September 2011.
- [14] —, "D1.2 Final GeoNet Specification," http://www.geonet-project.eu/?download=GeoNet-D.2.2_final.pdf, September 2011.
- [15] 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>
- [16] —, "Domain names - concepts and facilities," RFC 1034 (Standard), Internet Engineering Task Force, Nov. 1987. [Online]. Available: <http://www.ietf.org/rfc/rfc1034.txt>
- [17] 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.
- [18] Wikipedia, "IEEE 802.11p," September 2011. [Online]. Available: http://en.wikipedia.org/wiki/IEEE_802.11p
- [19] 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.
- [20] E. M. van Eenennaam, G. Karagiannis, and G. J. Heijenk, "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.
- [21] V. C. Harish and B. Owens, "Dynamic Load Balancing DNS," *Linux Journal*, p. 11, August 1999.
- [22] Wikipedia, "Haversine formula," September 2011. [Online]. Available: http://en.wikipedia.org/wiki/Haversine_formula
- [23] —, "geo," September 2011. [Online]. Available: <http://en.wikipedia.org/wiki/geo>
- [24] ICANN, "ICANN Approves Historic Change to Internet's Domain Name System," <http://www.icann.org/en/announcements/announcement-20jun11-en.htm>, September 2011.
- [25] Wikipedia, "Wireshark," September 2011. [Online]. Available: <http://en.wikipedia.org/wiki/Wireshark>