Connecting Vehicle Scatternets by Internet-Connected Gateways

Kendy Kutzner[1], Jean-Jacques Tchouto[1], Marc Bechler[2],
Lars Wolf[2], Bernd Bochow[1], Thomas Luckenbach[1]

February 14, 2003

Abstract

This paper presents an approach for interconnecting isolated clouds of an ad hoc network that form a scatternet topology using Internet gateways as intermediate nodes. The architecture developed is intended to augment FleetNet, a highly dynamic ad hoc network for inter-vehicle communications. This is achieved by upgrading FleetNet capabilities to establish a communication path between moving vehicles and the Internet via Internet gateways to facilitate direct gateway to gateway communications via the Internet, thus bridging gaps in the network topology and relaying packets closer towards their geographical destination at the same time. After outlining the overall FleetNet approach and its underlying geographical multi-hop routing, we focus on the FleetNet gateway architecture. We describe required modifications to the gateway architecture and to the FleetNet network layer in order to use these gateways as intermediate nodes for FleetNet routing. Finally, we conclude the paper by a short discussion on the prototype gateway implementation and by summarizing first results and ongoing work on inter scatternet communication.

1 Introduction

More and more vehicle manufacturers are interested in integrating wireless devices, communication and navigation facilities in their vehicles. Vehicles are expected to become a part of the Internet in the near future, either as a terminal in a mobile network, as a network node or as moving sensor (providing environmental, cars status or even video information) or a combination thereof. Moreover, interest of vehicles' passengers in location-based information is steadily growing. Drivers and passengers may like to receive information about traffic jams or accidents in their vicinity, or chat with other vehicle's passengers.

In order to accomplish this, vehicles can be equipped with short range radio hardware for inter-vehicle communication and make use of multi-hop communication. Due to the radio technology used the transmission range of each vehicle is about 1 km under line of sight conditions and much less in urban areas under fading and diversity conditions. Additionally, the density of equipped vehicles may vary for a given region, thus limiting the use of multi-hop communication. During the early deployment phase or in rural areas outside towns it may even reach densities close to zero. Thus, it is likely that there are groups of vehicles which can communicate, but no means exists to communicate between those groups. Such groups are commonly called scatternets. In such a scenario, there is a need to inter-connect those groups.

One option is to tunnel the traffic through other networks, for example through the Internet. For this reason one has to introduce gateways between the different types of

---

[1] Fraunhofer FOKUS

[2] TU Braunschweig

networks. These gateways are connected to the local ad hoc network clouds by radio links and to the Internet by other means. They have the ability to encapsulate data packets received on the radio link and tunnel them through the Internet.

This paper will give an overview of the FleetNet project in the next section. Section 3 will explain the approach for the mutual communication between vehicles, the Internet connectivity as well as the communication between clouds of vehicles. After this, section 4 will show some details of the prototype implementation of the Internet gateway, and section 5 will conclude by presenting preliminary results.

2 FleetNet – Internet on the Road

The FleetNet project [1] investigates the aspects of vehicle communication on the road. FleetNet was setup by a consortium consisting of DaimlerChrysler AG, FhI FOKUS, NEC Europe Ltd, Robert Bosch GmbH, Siemens AG, and the Universities of Braunschweig, Mannheim, Hamburg-Harburg and Hannover.[3]

The FleetNet objectives and challenges to achieve are:

- the enhancement of an existing UTRA-TDD[4] based radio communication system for ad hoc communication between high-velocity nodes;
- the development of a multi-hop vehicle communication system featuring position-aware ad hoc routing in a fast changing topology;
- the integration of FleetNet into the global Internet, enabling mobile FleetNet nodes to access the Internet and to provide services to Internet clients;
- the design of benchmark applications from fields of Cooperative Driver Assistance (improve driver safety), Decentralized Floating Car Data (collection and distribution of traffic information, weather conditions, traffic jam info), and Passenger Communication and Information (e.g., 'comfort' aspects and marketing along the road);
- the introduction of new low-cost communication options for vehicle's passengers;
- the regulatory issues and definition of market introduction strategies.

The FleetNet project will develop a communication platform for inter-vehicle communication, specify, simulate, verify and standardize the solutions found and implement the required architectural components and modules. It will further demonstrate the feasibility and the scalability of the approach by setting up a small scale demonstrator using a fleet of vehicles.

3 Technical Approach

Under low density conditions of FleetNet-equipped vehicles, FleetNet will form separated clouds of ad hoc networks subsequently called scatternets. Vehicles able to mutually communicate at a given point in time belong to the same scatternet. The FleetNet approach of multi-hop inter-vehicle communication is described in short in section 3.1. FleetNet introduces a gateway architecture providing vehicle-to-Internet communication, an introduction to the gateway architecture is given in section 3.2. These gateways are upgradeable in order to support scatternet connectivity as well. The idea of joining scatternets is set forth in section 3.3. An overview of the approach can be seen in figure 1.

---

[3] The project is partly funded by the German Ministry of Education and Research (BMB+F).

[4] UMTS Terrestrial Radio Access Network - Time Division Duplex

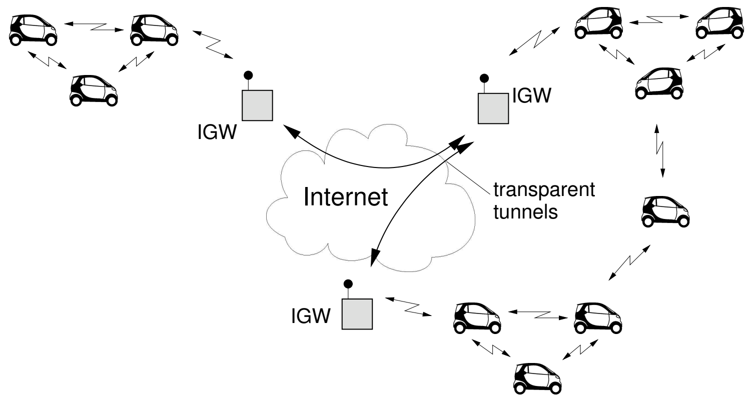

Figure 1: Assumed Configuration

3.1 Intra-Scatternet Communication

The nodes within the scatternet are composed of moving vehicles, thus the topology is highly dynamic, especially for high velocity nodes. The communication is self-organized, wireless and forms a rapidly changing ad hoc network. In order to allow communication distances larger than the radio range, data packets will be forwarded by other vehicles (intermediates nodes). The primary function of an intermediate node in the scatternet is to accept packets from a source node and to deliver them towards the destination node. To accomplish this, a route through the scatternet must be determined. Generally, more than one route is possible. Thus, a routing function must be executed and must fulfill the following design characteristics:

- low control overhead,
- low packet delivery delay and high delivery rate.

In turn, these characteristics are preconditions for scalability and adaptability.

The appropriate routing protocols to be applied within the scatternet are currently investigated [2] and implemented within the FleetNet project. The routing protocol within the scatternet is position-based. Position-based routing protocols consist of two main parts: a location service and a geographical forwarding part. The geographical forwarding protocol used within the scatternet can be summarized with the following points:

- Nodes (vehicles) are addressed with their actual location and a node ID;
- Routing is performed on a per packet basis. A next hop is chosen for each packet arriving at a node (packet forwarding);
- Destination and neighborhood locations are sufficient for the routing decision;
- The packet headers carry ID and location of source and destination.

Each vehicle within the scatternet is supposed to be equipped with a GPS receiver, so it is possible for a vehicle to know its actual geographical position. A location service is used by a sender of a packet to determine the position of the destination and to include it in the packet's destination address. Once the location of the destination is acquired, a node may transmit its packets to the destination using geographical forwarding.

3.2 Gateway Architecture

A very interesting feature in FleetNet is the access to the Internet via roadside-installed Internet Gateways (IGWs). These IGWs appear as common (but stationary) nodes in the FleetNet radio ad hoc network providing a connection to the Internet. Hence, vehicular-based applications will benefit from this option as they are not limited to their local scope

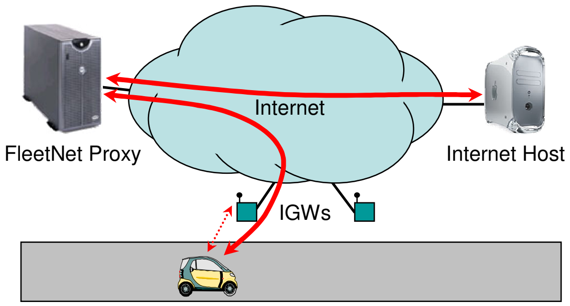

Figure 2: MOCCA's Proxy-Based Communication Architecture

only, but can utilize information and resources from the Internet. However, FleetNet's communication system differs in several aspects from fixed IP-based networks, which prevents the interoperability with Internet communication protocols. In order to handle these differences, we developed MOCCA (MObile CommuniCation Architecture), a communication architecture that integrates FleetNet into the Internet.

3.2.1 MOCCA's Communication Architecture

In FleetNet, the FleetNet Network Layer (FNL) provides access to the communication system. FleetNet uses a FleetNet ID to address a vehicle uniquely. Moreover, the FNL deploys the location-based routing and forwarding scheme as described previously. In order to achieve interoperability with the Internet, we have to attach an IP layer upon the FNL. The differences are handled by an adaptation layer within the FNL, the FNA (FleetNet Adaptation, cf. figure 3). For an IP-based addressing of vehicles, the FleetNet IDs exceed the 32 bit address space of IPv4 easily. Hence, we use IPv6 addresses in FleetNet since their 128 bit length provide sufficient capacity. The FNA assembles a vehicle's IPv6 address using the FleetNet ID for the lower part. A global IPv6 "FleetNet prefix" represents the upper portion of this address. Hence, the FleetNet communication system appears as one complex IPv6 subnet from a conceptual point of view. In analogy to classical ad hoc networks, we decided not to deploy any addressing hierarchies within the IPv6-based vehicular ad hoc network. Due to the high mobility of the vehicles, it seems almost impossible to maintain such hierarchies without causing noticeable overhead.

In order to integrate the IPv6-based FleetNet into the IPv4-based Internet, MOCCA deploys a proxy-based communication architecture (figure 2). One key element in MOCCA is the FleetNet Proxy. From the communication protocols' point of view, the FleetNet Proxy brings together the different communication protocols from FleetNet and the Internet. The FleetNet Proxy may be hosted by an arbitrary Internet provider. Of course, there will be several FleetNet Proxies in the final deployment, e.g. hosted by different vehicle vendors or OEM suppliers. In order to enable IPv4-IPv6 interoperability, we deployed NAT-PT (Network Address Translation – Protocol Translation, RFC 2766) in the FleetNet Proxy. NAT-PT enables a transparent translation between IPv4 and IPv6 addresses and, thus, provides the most flexible solution for our purposes (cf. figure 3). MOCCA's network layer also has to take care for mobility aspects, which is detailed in section 3.2.2.

Figure 3 summarizes the mechanisms and protocols on the different communication layers. Communication between the IGW and the vehicle bases upon the FleetNet communication layers, i.e. the FleetNet Physical (FPHY), FleetNet Data Link Control (FDLC), FleetNet Network Layer (FNL), and FleetNet Adaptation (FNA). For efficient communications, the FleetNet Proxy divides the end-to-end connection into two segments: Communication between an Internet host and the FleetNet Proxy, and between vehicle and FleetNet Proxy (via an IGW). Note that the FleetNet Proxy covers both the network layer and the transport layer. At the transport layer, MOCCA deploys an optimized FleetNet Transport

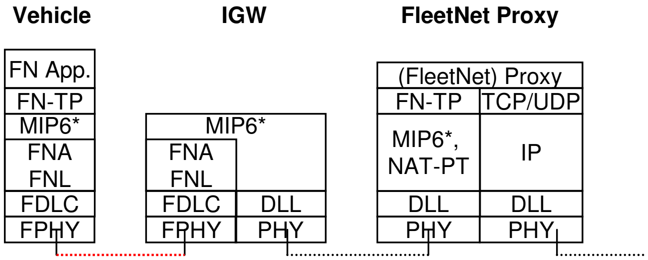

Figure 3: Protocol Overview in MOCCA

Protocol (FN-TP) for efficient communications. Hence, we intentionally violate the end-to-end semantics in favor of communication efficiency. The FN-TP is detailed in [3].

3.2.2 Mobility Support in MOCCA

If an Internet host (CN, correspondent node) wants to communicate with a vehicle, it has to find a route to the vehicle via a respective IGW. Hence, we need a solution to handle the vehicles' mobility in the fixed Internet. In MOCCA, we combined our proxy-based communication architecture with Mobile IP. The home agent (HA) thereby represents a vehicle's (global) IPv6 address. The FleetNet Proxy plays an important role, because it maintains the HAs of the FleetNet-enabled vehicles. From a logical point of view, the IGWs function as foreign agents (FAs), and the vehicles themselves represent the mobile nodes (MNs). Hence, data sent from an Internet host to the vehicles will be always routed to the HA at the FleetNet Proxy. The HA tunnels the data to the FA the vehicle is currently registered with. Finally, the FA unpacks the data packets and forwards them to the MN via the vehicular ad hoc network.

For MOCCA, we developed Mobile IPv6* (denoted as MIP6* in figure 3). Mobile IPv6* is an optimized Mobile IP for FleetNet, which differs in several aspects. As stated previously, FleetNet relies on the global IPv6 addresses only. Hence, Mobile IPv6* consequently avoids any overhead caused by link-local address assignment, router advertisement/solicitation, and neighbor discovery defined for IPv6-based networks. Another important difference are co-located care-of addresses. This mandatory feature in Mobile IPv6 supersedes the FA. A MN will always receive such a (link-local) co-located care-of address in the foreign network. The MN then updates this information to the previous access router, the HA, and current CNs ("binding update"). However, this feature causes additional overhead in the FleetNet radio ad hoc network. For example, data will be tunneled in the ad hoc radio network if a handoff occurs. In order to avoid this overhead, we re-introduced FAs located on the IGWs in Mobile IPv6*. Hence, MNs register themselves explicitly with the FAs as described in Mobile IPv4 (RFC 3220).

However, using Mobile IP for handling mobility in ad hoc networks is generally not possible. A MN always requires an immediate link to its FA. Mobile IPv6 therefore uses link-local IPv6 addressing for its router advertisements. However, in ad hoc networks like FleetNet, each MN acts as a router for relaying packets. As a result, a MN would select an arbitrary adjacent MN for its default gateway instead of an IGW. In order to overcome this problem, we identify IGWs using DRIVE (DiscoveRy of Internet gateways from VEhicles), a service discovery protocol for MOCCA. DRIVE's very basic concept is the passive discovery approach. Classical service discovery protocols (e.g., Service Location Protocol, UPnP, Salutation [4]) discover their environment actively. If a device (the so-called user agent) seeks for a service, it will query the network (or a central instance) for this service and will receive a response from the service provider. However, this approach does not scale with the number of vehicles in FleetNet's highly dynamical ad hoc network. Hence, DRIVE transposes the roles of service providers and mobile devices seeking a service. The

IGWs therefore announce their service periodically in a restricted geographical area. A vehicle receiving the announcements stores them in a local database. A user agent within the vehicle only needs to query the local database instead of the overall network. A simple example is the "Foreign Agent Configurator", an user agent that queries the local database for new IGWs and reconfigures Mobile IPv6* accordingly to use this IGW as its new FA. DRIVE scales well as the overhead increases with the number of IGWs basically and not with the number of FleetNet-enabled vehicles [5]. Section 4 provides an overview of DRIVE's implementation.

3.3 Inter-Scatternet Communication

The presence of a gateway architecture as described above leads to the idea of connecting otherwise separated scatternets via the Internet. FleetNet IGW's currently support gateway-to-gateway communications only via the associated FleetNet Proxy. Since one of the most promising features of FleetNet is in the low delay of inter-vehicle communications, a direct gateway-to-gateway connection for bridging the gap between scatternets would greatly enhance FleetNet's availability. Additionally, otherwise lost geographical information will be preserved.

Hence we introduce the option of direct inter-scatternet communication via gateways. Data packets arriving at a gateway which are not addressed to an Internet host will be tunneled to another gateway closer to the destination. This allows to use geographical routing and geographical addressing in a much broader scope, but for it to work protocol stacks in the gateways and in the vehicles have to be modified.

Since the suggested inter-scatternet communication is an extension to existing FleetNet protocols, only minor changes are necessary. Proposed modifications are depicted in figure 4.

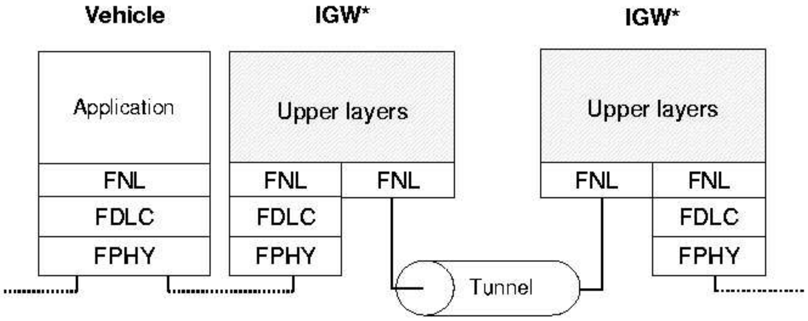

Figure 4: Protocol Overview for Gateway-to-Gateway Communication

As can be seen in figure 5, FleetNet geographical routing algorithms are still in place. However, there are a few changes concerning the selection of a gateway-to-gateway routing option.

1. Since geographical routing might fail, e.g. in case of net partitioning, the node detecting the failure can decide to route the data packet to the next known gateway instead of dropping the packet.

2. The source or any intermediate node estimates the hop count required to reach the destination. If the expected hop count exceeds a given limit, it is assumed that gateway-to-gateway routing will reduce the number of hops required significantly. In this case packets are routed to the next gateway by the means of geographical routing.

3. After the gateway-to-gateway routing is completed, geographical routing is resumed. Subsequent gateway-to-gateway routing is not an option, since routing loops will occur. If geographical routing fails this time, the packet cannot be delivered.

Clearly, the gateway-to-gateway routing option makes sense only if a gateway is available within a reasonable geographical distance from the source.

Because gateway-to-gateway routing allows to significantly reduce the number of hops required due to the fact that they can bridge larger distances, the probability of successful packet delivery is increased [6]. A useful threshold value needs to be determined with respect to the gain expected in terms of hop count reduction, reduced packet loss rate, and expected packet delay variation.

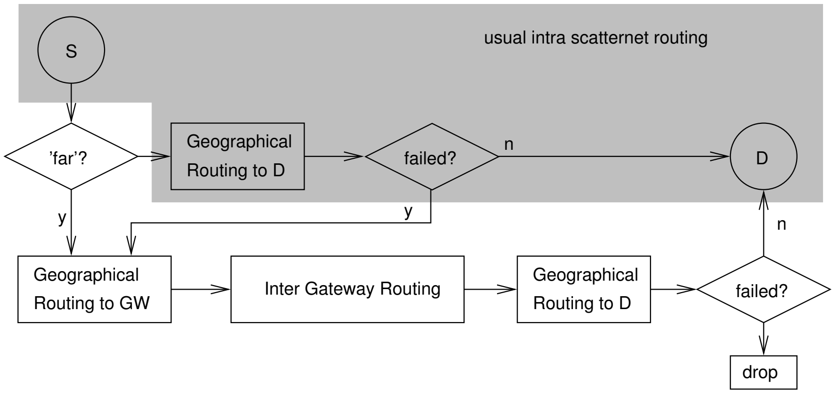

Figure 5: Forwarding Strategy using Gateway Communication

Ordinary nodes rely on a beacon broadcast announcing their presence and geographical position to establish one hop connectivity. Internet-wide broadcast in order to announce the presence of gateways is not possible for obvious reasons. To circumvent this, each IGW is required to distribute a table of other IGW's known to every member of this table. The table of known gateways consists of (IGW-ID, IP address, location) tuples and of course includes the originating IGW. Since the number of gateways is unknown and expected to be large, reducing the table size is mandatory. A full size table would correspond to a fully meshed gateway topology, therefor reducing the table size will introduce multi-hop gateway-to-gateway routing. For this purpose, the following algorithm is proposed:

1. Divide the whole area of operation into n subareas.
2. Select one Gateway in each subarea, where this IGW is not included. If more than one IGW is available for selection, the one with the closest ID is chosen like in [7].
3. Further divide the subarea that includes this IGW.
4. Start over at 2, if the level of subdivisions is smaller than a given threshold m.
5. Publish the resulting table to all members of the table.

This algorithm ensures not only local connectivity but also guarantees that all IGWs will have long-range neighbors. Memory requirements for saving the location of all selected neighbor gateways are reasonable, and depends on n and m. Herein n specifies the number of subdivisions and therefore the degree of connectivity between gateways. It is expected to be a square number. The maximum number of hops in gateway-to-gateway routing is given by m.[5] The required table size then is $m \cdot (n-1)+1$. As this number

---

[5] Let x be the size of the area of operation in one dimension and d the distance to the nearest gateway, then $\frac{x}{\sqrt{n}^m} \approx d$ or $m \approx \log_{\sqrt{n}} \frac{x}{d}$. For example if $x = 40000$km (length of equator), $d = 1$km and $n = 4$ then the nearest integer m would be 15.

grows only with the number of subdivisions and not with the number of gateways, it scales very well.

Routing between IGWs relies on the same geographical forwarding schemes as used for vehicular nodes: Each packet is forwarded to the neighbor closest to the destination. If no other known IGW is closer to the destination, gateway-to-gateway routing is completed and the data packet is forwarded to the next vehicular node.

As pointed out in section 3.1, it is necessary for a source vehicle to be able to determine the geographical location of a destination vehicle prior to any data transfer. This also applies if nodes are located within different scatternets. Therefore, a location service must be active across gateway boundaries. Many location service schemes proposed (including for example [7]) only presume that geographical routing can be applied. Since this is valid for the gateway-to-gateway routing scheme described herein, a location service will successfully operate via gateway-to-gateway routing.

4 Prototype Implementation of the Internet Gateways

For our investigations, we developed a prototype of an Internet Gateway. Our platform bases on the Linux operating system. An IGW has to perform the following basic protocol mechanisms: First, it has to provide the FA functionality of Mobile IPv6*. Second, the IGW is an integral part of DRIVE. Our Mobile IPv6* implementation bases upon the DYNAMICS implementation of Mobile IPv4 (from Helsinki University of Technology). We therefore implemented the respective IPv6 support in DYNAMICS for the deployment in FleetNet. The extension of Mobile IPv4 was easier compared to the implementation of the FA functionality for an existing Mobile IPv6 implementation.

For the implementation of DRIVE, we built upon OpenSLP, a freely available implementation of the Service Location Protocol (SLP, RFC 2608). DRIVE deploys IPv6 technology, too. However, it is not in accordance with the IPv6-based specification of SLP (RFC 3111), which does not support DRIVE's passive discovery concept. Like OpenSLP, DRIVE's implementation consists of two components: a SLP daemon (`slpd`) and a SLP library (`libslp`), as illustrated in figure 6. In order to enable the proactive service announcements, we divided the `slpd` in two functional units: an IGW SLP daemon, and an in-vehicle SLP daemon. A beacon generator within the Internet Gateway triggers the IGW SLP daemon to announce service advertisements (`SAAdvert`) periodically. The IGW SLP daemon uses the location-based addressing of the FleetNet Network Layer, which enables the specification of an area in which the service advertisements are propagated. The `SAAdverts` messages comprise a Service URL indicating the IPv6 address of the IGW, and a list of several attributes describing the IGW's current state parameters. We currently support the following four attributes:

- `x-fn-users`: the number of vehicles that are registered with the IGW
- `x-fn-bandwidth`: the bandwidth currently available
- `x-fn-timestamp`: a timestamp to differentiate the IGW advertisements transmitted (derived from GPS)
- `x-fn-commercial`: specifies an URL provided by the IGW provider for announcing marketing information

Within the vehicle, the in-vehicle `slpd` receives the service advertisements and stores the extracted information in a local database. If an application wants to discover an IGW, it queries the (local) in-vehicle `slpd` using functions from `libslp` (dotted arrows in 6. The `libslp` sends a service request (SrvRqst) message to the in-vehicle `slpd`. The `slpd` then searches the local database for a respective IGW and responds the result in a service reply (SrvRply) message. This discovery process within the vehicle corresponds to the service discovery in SLP exactly. Hence, modifications to the user agent's functionality

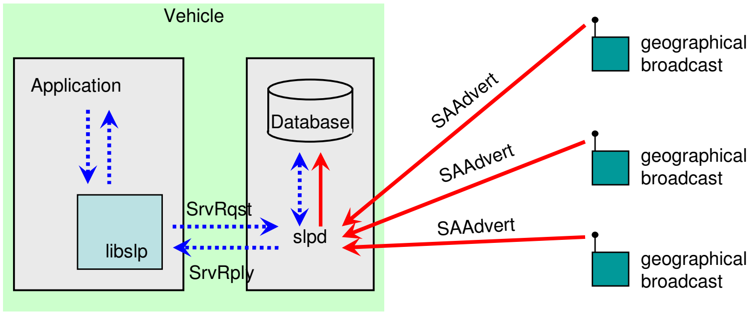

Figure 6: Structure of DRIVE's Implementation

are not required. For example, a simple "Marketing Along the Road" application querying for an IGW will receive the IGW currently available together with its attributes. This application analyzes the `x-fn-commercial` attribute, and opens a WWW browser with the URL specified in this attribute.

5 Conclusion and Future Work

In the previous sections we described the FleetNet approach focusing on the FleetNet to Internet gateway architecture. We presented an approach for upgrading Internet gateways to support direct gateway-to-gateway communications via the Internet. This allows to bridge gaps in the network topology resulting from a low density of FleetNet-equipped vehicles that will likely cause the underlying FleetNet vehicle-to-vehicle routing to fail.

It has been shown that a minor modification to the FleetNet network layer accompanied by an upgrade of the FleetNet gateway architecture will allow to relay packets closer towards their geographical destination via Internet-connected gateways. This approach can be used to either bridge gaps in the ad hoc network as well as establishing shortcuts in FleetNet multi-hop routing, thus reducing the number of hops required to reach the geographical destination. It is expected that this will result in an enhanced performance of FleetNet under low penetration conditions.

The proposal presented in this paper is currently under performance evaluation. Nevertheless, a number of open issues still exist, e.g.:

- How does an IGW obtain the initial set of neighboring gateways in order to set-up a hierarchical geographical neighbor table?
- How is a threshold determined efficiently for each data packet in order to select gateway-to-gateway routing rather than vehicle-to-vehicle routing?
- How can addressing schemes such as geographical broadcast be preserved across IGW's?

Clearly, possible solutions must not rely on any assumptions regarding network topology or the availability of centralized servers since either gateways and vehicles participate in a self-organizing, non-managed and fast-changing ad-hoc network. But it seems that e.g. FleetNet proxies can be utilized to provide information about neighboring gateways, and that gateway-to-gateway multicast might allow for geographical broadcast schemes to a scatternet topology.

References

[1] FleetNet homepage, 2003. `http://www.fleetnet.de`.

[2] M. Mauve, J. Widmer, and H. Hartenstein. A survey on position-based routing in mobile ad hoc networks. *IEEE Network Magazine*, 15(6):30–39, November 2001.

[3] Marc Bechler, Walter Franz, and Lars Wolf. Mobile Internet Access in FleetNet. In *13. Fachtagung Kommunikation in Verteilten Systemen, Leipzig*, February 2003.

[4] C. Lee and S. Helal. Protocols for Service Discovery in Dynamic and Mobile Networks. In *International Journal of Computer Research, Special Issue on Wireless Systems and Mobile Computing*, 2002.

[5] Marc Bechler, Oliver Storz, Walter Franz, and Lars Wolf. Efficient Discovery of Internet Gateways in Future Vehicular Communication Systems. In *Proceedings of the 57th IEEE Semiannual Vehicular Technology Conference, Jeju, Korea*, April 2003.

[6] Brad Karp and H. T. Kung. GPSR: greedy perimeter stateless routing for wireless networks. In *Mobile Computing and Networking*, pages 243–254, 2000.

[7] Jinyang Li, John Jannotti, Douglas S. J. De Couto, David R. Karger, and Robert Morris. A scalable location service for geographic ad hoc routing. In *Proceedings of the 6th ACM International Conference on Mobile Computing and Networking (MobiCom '00)*, pages 120–130, Boston, Massachusetts, August 2000.