

Thoughts on a Protocol Architecture for Vehicular Ad-hoc Networks

Holger Füßler*, Marc Torrent-Moreno[†], Matthias Transier*, Andreas Festag[‡], and Hannes Hartenstein[†]

*Computer Science IV, University of Mannheim, Germany
 {fuessler,transier}@informatik.uni-mannheim.de

[†]Institute of Telematics, University of Karlsruhe, Germany
 torrent@tm.uni-karlsruhe.de, hartenstein@rz.uni-karlsruhe.de

[‡]NEC Deutschland GmbH, Germany
 festag@netlab.nec.de

Abstract— In comparison to other communication networks, Vehicular Ad-hoc Networks (VANETs) have unique requirements with respect to applications, types of communication, self-organization and other issues. In order to meet these requirements, the structuring of functionalities into protocols and their interaction must be re-thought. The traditional approach of decomposition of functionality into protocol layers (*layered* approach) and a protocol design specifically tailored to the needs of VANETs (*un-layered* approach) leads to two extreme and opposed manifestations of a potential VANET protocol architecture. From these two extreme approaches we derive a stack-based VANET protocol architecture that combines the strengths of both. Among the key features of this protocol architecture are VANET-specific protocol layers, a staircase approach for interaction among layers, and the use of an information connector for the exchange of cross-layer information using the publisher/subscriber pattern. This protocol architecture provides a clear modular structure with flexibility for protocol interaction and information exchange at a reasonable complexity.

I. INTRODUCTION

Previous and current research, development, and deployment projects [1], [2], [3], [4], [5] and standardization efforts [6], [7], [8] show the great interest in Vehicular Ad-hoc Networks (VANETs). VANETs are a special kind of Mobile Ad-hoc Networks (MANETs) and are characterized as follows:

Wide spectrum of applications: VANETs can be used in many applications for vehicle-to-vehicle and vehicle-to-roadside communication, as opposed to networks that are tailored to specific applications as are most of existing sensor networks. In addition, the technology might be used to connect to a home network when the car is in the garage.

However, the focus of deployment of this technology in cars will most likely be vehicular safety applications

Holger Füßler, Marc Torrent-Moreno, and Andreas Festag acknowledge the support of the German Ministry of Education and Research (BMB+F) as part of the Network-on-Wheels (NoW) project under grant no. 01AK064F

with specific requirements for simultaneous reliability and timeliness.

Type of communication: Whereas conventional network applications use uni- or multicast communication, i.e., communication where endpoints are identified by unique system or group IDs, safety applications—the focus of government-funded projects dealing with VANETs—typically address geographical areas in which data needs to be distributed.

Self-organization and -management: Like MANETs in general, a VANET requires fully decentralized network control since no central entity could or should organize the network. Moreover, VANETs hold an additional complexity due to special conditions (i.e., the above-mentioned timing and reliability requirements, together with probable saturation when VANET technology is fully deployed).

Interaction with on-board sensors: A VANET platform will most likely include on-board sensors like GPS, to be utilized not only by applications, but also by network protocols, e.g., by position-based routing [9].

While there are even more facts that can be cited to describe the specific nature of VANETs compared to other wireless or ad-hoc networks, the above list appears to be sufficient to motivate the need for a specific VANET protocol architecture.

Well-known layered protocol architectures like those in OSI [10] or the Internet [11] have proved to be very useful for traditional (wired) networks. The assumption of protocol layering being the pertinent abstraction leads to the attempt to adapt the traditional protocol stack to the needs of VANETs. In this approach, the principal assignment of functionality to the protocol layers, i.e., covering almost all layers of the OSI reference model, remains. Existing layers must be extended by additional functionalities which are specific to VANETs.

Alternatively to the traditional layering approach, another organizational principle for protocol functionality is needed. One approach is to tailor the VANETs specifi-

cally to vehicular safety as the main target application. In this approach, there would be a single block responsible for communications that would try to satisfy safety application requirements along with having the complex task of controlling the access to the medium.

We consider both approaches as two extreme cases of a potential network architecture for VANETs. Analyzing both approaches with respect to their benefits and weaknesses, we advocate a protocol architecture that combines the advantages of both.

Related Work: Numerous papers discuss the structuring of network protocols, ranging from wired to cutting-edge wireless networks. The dominant protocol architecture used in common computer systems today is TCP/IP [11]; another reference model, often used for education, is the ISO/OSI model [10]. Since traditional approaches also have their limitations in solving various network problems, there are some efforts to tackle these problems with new architecture proposals. Protocol Heap [12], Flexible Protocol Stacks [13], and Sensor Stack [14] are such approaches which were very inspiring to this work. In addition, many research and standardization efforts deal with the topic of Vehicular Ad-Hoc Networks [1], [2], [3], [4], [5], [6], [7], [8] or Mobile Ad-Hoc Networks [15]. Due to space restrictions, we will not discuss their protocol architectures in this paper.

The remaining part of the paper is organized as follows: We first provide in Sect. II several observations found in VANETs that motivate us for this work. In Sect. III we will describe the two extreme cases of protocol design, i.e., the traditional *layered* approach and the *un-layered* approach that is not restricted in the presence of layers and cross-layer interactions, derive our architectural proposal and explain how the architecture better fits to the observations made. Finally, we will present the conclusions of our work.

II. OBSERVATIONS

We provide in the following section several observations from which we will derive our architecture proposal.

Relationship to sensor networks: While the notion of sensor networks usually stands for (non)-mobile wireless networks with low-power and low-capability devices distributedly gathering sensor information, there are some important similarities between sensor networks and VANETs that might influence architectural considerations. First, a vehicle can be seen as a high-capability sensor device with sensors for environmental information such as road grip or temperature, and for information about the vehicle itself such as movement. Second, the sensor information coming from different vehicles en route can be combined in order to eliminate

redundancy, minimize the number of transmissions, and improve the quality of the sensor information. This ‘data centric routing’, as opposed to ‘address-centric routing’, is well known from sensor networks (e.g., [16], [17]). In addition, the whole communication system might react to sensor information in the sense that sensor events are an integral part of network protocols. However, the main difference between VANETs and classical sensor networks is most likely that for VANETs, the main goal of these protocols is not the preservation of energy but a ‘low channel utilization’ to keep the system accessible for urgent safety messages.

Packets vs. information: Along the lines of the first observation, one has to differentiate between ‘packets’ and ‘information’: In classical networks, the data payload of a packet is meant to be delivered unchanged to the addressed application instance(s). However, VANET applications will most likely evaluate the information contained in a packet, merge it with their own state and then decide how to communicate this updated information. This operation is known as ‘in-network’ processing.

End-to-end notion revisited: In a traditional network, peer application and protocol entities are well-defined on all ‘communication endpoints’—either by an ID or by a multicast group. However, the VANET communication entities might not only address specific peer entities, but also geographical or topological areas whose members are likely to change over time. Furthermore, a communication between two peers might only be possible in one direction but not vice versa.

Network protocol requirements: Among other things, the last observation directly leads to different requirements for multi-hop packet-forwarding protocols. On the one hand, traditional unicast and multicast protocols using ID-based addressing might still be needed for infotainment applications or the extension of hotspot access. On the other hand, the challenge for VANET network protocols lies in efficient geocasting and flooding. Additionally, there might be potentially severe requirements concerning reliability and/or timeliness due to the safety purpose of some applications.

Granularity of control: In classical network management, the control parameters are set as ‘mid-term’ or ‘long-term’ parameters. E.g., the setting of an IP address tends to be long-term and even in UDP communication sessions packet options are usually changed for every session (mid-term) but not for single packets within one session. In a VANET, however, it seems that various control parameters will have to be set on a per-packet basis, as when sending successive packets different MAC algorithms could be used, different transmission powers could be set, or the packets could be sent to different physical channels.

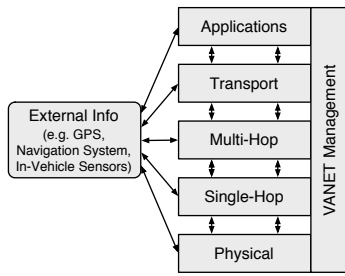


Fig. 1. Layered Approach

Information sharing: In a VANET, the communication system generates information that is of high value to many protocol entities. Beacon packets could be used to generate a list of neighboring nodes, that could be used both for driver assistance *and* packet forwarding decisions. Thus, we observe the need to share information in an efficient and clean manner without creating complex control interactions. In addition, the integration of these events into protocol state machines demands a standardized means to access them, if implementation portability is desired.

Application requirements vs. medium conditions: The safety-focused nature of VANETs requires the communication system to be dependably able to deliver important packets. To achieve this, the packets have to contend with (a) the sending demands of other nodes and (b) the allocation of the radio channel by other nodes. In addition to that, the channel itself is highly probabilistic [18]. Thus, in order to meet application requirements, not only will all nodes have to cooperate among themselves but also all applications and protocols on a single node.

III. ARCHITECTURE

In general, a protocol architecture achieves interoperability for communication among network nodes and provides the framework for implementation. In designing the communication suite for VANETs, two approaches can be taken.

First, following the traditional approach, the overall functionality could be de-composed and organized in layers such that the protocols fulfill small, well-defined tasks and form a protocol stack as in TCP/IP [11] and ISO/OSI [10]. Second, one could try to build a customized solution to meet the requirements of VANETs. With such a non-layered, but still modular approach we are not restricted to the assignment of functions to particular layers and their limited layer interactions. In the following, we will describe both—fundamentally feasible but extremely opposite—approaches and briefly outline their advantages and disadvantages. Afterwards, having learned the benefits of both systems, we will describe a third approach and argue why we think this

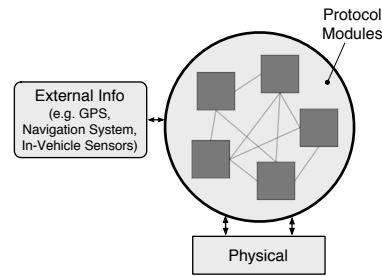


Fig. 2. Un-layered Approach

protocol architecture would be better suited for a VANET system.

The first approach—called a *layered approach* and depicted in Fig. 1—attempts to retain the order of functions and protocol layers with well-defined interfaces between them. It adapts system functionalities to the needs of a VANET communication system, resulting in protocol layers for single-hop and multi-hop communication. The limitations and inflexibility of traditional network stacks when used in ad-hoc networks are well known (see related work part of Sec. I). Each layer is implemented as an independent module with interfaces (SAPs) only to the adjacent above and below layers. Consequently, protocols can not easily access state or meta-data of a protocol on a different layer, which makes data aggregation difficult. Moreover, some VANET-specific functions, such as those for network stability and control, do not fit into the traditional layered ISO/OSI model and cannot be uniquely assigned to a certain layer. It is also worth noting that every layer accesses external information separately with no common interface, which might lead to problems when this information influences protocol flow.

The second, *un-layered approach* would be the result of tailoring a whole new system to the needs of VANETs' main focus, i.e., safety applications. Having accurate specifications of these applications and the willingness to use the 'probabilistic' channel in the most efficient manner leads to having a highly coupled set of protocols. Therefore, all application and communication protocols are placed in one single logical block right over the physical interface and connected to the external sensors (Fig. 2). Inside this block, all protocol elements are modularized such that there are no restrictions on interaction, and state information is arbitrarily accessible. Note though, that due to arbitrary and complex interactions of their modules this 'architecture' inherits a high design complexity. This makes protocol specification a complicated matter and so, once designed, it becomes an extremely inflexible system for other types of application (e.g., it would be difficult to integrate IP applications). Also it would be tough to systematically avoid control loops, which is rather easy in the layered approach with its clean top-down or bottom-up packet traversal.

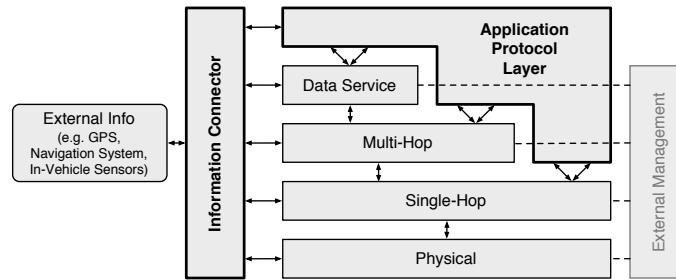


Fig. 3. Sketch of VANET Architecture

While both approaches would certainly be feasible, each has strengths and weaknesses with respect to assignment of functions, information sharing, flexibility, complexity, and other VANET-specific requirements. In summary, the un-layered approach may lead to an unacceptable degree of complexity in terms of interactions among the modules and of inflexibility when trying to combine it with other types of applications. The traditional layered approach is potentially too restrictive with respect to assignment of functionality, protocol interaction, and exchange of state information inside a stack.

Fig. 3 presents a concept in between the two ‘extreme’ options discussed above. In this proposal we intend to use the most adequate features of both options, i.e., (a) having a layered approach that gives us a clear and modular structure in which to build our applications and protocols, but also offering (b) a clean way of sharing information and to cooperate between any protocol module on any layer as needed.

Describing our proposal, we identify the following key features:

Presence of layers: To alleviate a structured protocol design, we use the same core structure as in the layered approach. We believe that the original meaning of each layer is still valid for VANETs, however, modifications/extensions are required. Note that the traditional ISO/OSI names have been replaced in each layer to give a better understanding on what has to be handled and to avoid confusion with the traditional TCP/IP approach.

Staircase approach: An application can select from among multiple service access points to lower layers. Depending on its requirements, an application can choose whether to use or to bypass a service offered by a lower layer, logically expressed by a staircase shape. This is in contrast to the traditional ISO/OSI protocol architecture, where applications can only access the directly adjacent layer. Our proposal offers more flexibility to send packets, though the standard path for outgoing packets will still be top-down through the layers accessing the available service access points (SAPs) [10] of adjacent layers. When a data packet traverses the stack bottom-up, every protocol layer has to decide whether the packet

should be given to the next higher protocol layer or to one or more application protocols. A packet header element such as a port/protocol number is required to allow for multiple applications.

Information connector: All protocols can connect to an ‘information connector’, i.e., a common interface that efficiently exchanges sensor update information, data extracted from packets, and state information (and their change) of protocol layers and devices. The information crossbar basically follows a publisher/subscriber pattern: Published information services can be subscribed by any entity. The information connector maintains information collected from each authoritative source and asynchronously notifies subscribers of matching information. It is worth noting that the information connector is not meant to write to the state in protocols and that it contains very volatile data due to its highly dynamic context. If and how protocols react to this information is left up to them.

External management plane: The external management plane symbolizes a configuration interface to set long-term system settings. In the sense of this proposal, it is not involved in the dynamic self-organization motivated by the different network conditions.

Having discussed the rough structural parts of the architecture, we want to quickly describe the meaning of the layer names and list some protocol functionality that would be part of those layers. The *single-hop layer* incorporates all functionality dealing with communication to direct radio neighbors. In addition to traditional MANET link layer functionality, there will be a protocol element that adds the node’s position to every packet. Also, a stability element will ensure that the single-hop communication adapts to channel and load conditions. The *multi-hop layer* contains protocol elements for forwarding packets to non-neighbor nodes, using neighbors as forwarders. Geocast is the main protocol on this layer in addition to traditional multi-hop protocols. The *data service layer* represents the rest between multi-hop packet-forwarding and the application. A datagram protocol interface or protocols providing a reliable byte stream and building on top of the multi-hop layer would reside here.

After having described the key features and main protocol elements of the system, we will now try to argue why we think that this meets the observations in Sec. II. One fundamental observation was the necessity to integrate sensor information into the local protocol work flow. This is achieved by the information connector, offering an interface to both protocol entities and sensors to publish and subscribe to events such as ‘Position Update Events’ or ‘Neighbor Position Change Events’. These events not only provide a clean and potentially portable interface for sharing information, they also address most of the ‘cross-layering’ issues occurring in recent protocol proposals. We also believe that the information symmetry alleviated by this interface plays a crucial role in the system’s capability to organize itself. The main entity taking care of network stability is a protocol element on the single-hop layer that serves as a bottleneck to all packets heading for the wireless link and is thus able to control the packet flow based on its queue *and* the information gathered by the information connector. This stability control entity is responsible for managing the best strategy and controlling the physical layer for every single packet in order to combat not only critical application requirements like timeliness/reliability but also expected severe channel conditions. On the other hand, we believe that the main responsibility for incoming safety-related packets resides in the corresponding applications. They will decide the best scheme to relay the information, and, if needed, aggregate it with previous knowledge gained from other messages or from the car’s own sensors. However, when a packet is only forwarded, the information contained in it—such as the position of the last forwarder—is offered to the information connector.

IV. CONCLUSIONS

Based on observations made for VANETs, we have proposed a protocol architecture that fits their needs. While the fundamental protocol organization is still layered and the path of a packet is still vertical through the layers, an information connector provides a clean interface to allow the sharing of information between protocol entities on every layer and additional sources of information like sensors. Furthermore, we have named and defined the respective layers and provided a list of protocol features that are likely to reside on them, and acknowledge the increased importance of per-packet control.

Analyzing the strengths and weaknesses of two extreme cases for protocol architectures, we believe that our moderate approach overcomes the limitations of traditional protocol architectures like ISO/OSI or TCP/IP with respect to the assignment of functions to protocol layers and cross-layer communication. With respect to

custom un-layered architectures, it avoids complex interactions among the modules, adds flexibility to support further applications, and provides a meaningful structure for standardization and the development of portable applications. Simultaneously, we retain the principle of protocol layers but with considerably enhanced cross-layer interaction for better network stability and control in VANETs.

We are in the process of implementing parts of the architecture for a ‘proof of concept’. In addition, we investigate how security and Internet access as additional important requirements fit into our architectural model.

REFERENCES

- [1] “The FleetNet Project,” <http://www.fleetnet.de>.
- [2] “The Network-on-Wheels Project,” <http://www.network-on-wheels.de>.
- [3] “The PATH Project,” <http://www.path.berkeley.edu>.
- [4] “The PReVENT Project,” <http://www.prevent-ip.org>.
- [5] “The DSRC Project,” <http://www.leearmstrong.com/-DSRC/DSRCHomeset.htm>.
- [6] “IEEE 802.11p Task Group,” <http://grouper.ieee.org/-groups/scc32/dsrc/index.html>.
- [7] “Car2Car Communication Consortium,” <http://www.car-to-car.org/>.
- [8] “Internet ITS,” <http://www.internetits.org>.
- [9] H. Füller, M. Mauve, H. Hartenstein, M. Käsemann, and D. Vollmer, “A Comparison of Routing Strategies for Vehicular Ad Hoc Networks,” Department of Computer Science, University of Mannheim, Tech. Rep. TR-02-003, July 2002.
- [10] B. N. Jain and A. K. Agrawala, *Open Systems Interconnection: Its Architecture and Protocols*. Elsevier, 1990.
- [11] E. W. Meyer, Jr., “RFC 46: ARPA network protocol notes,” Apr. 1970.
- [12] R. Braden, T. Faber, and M. Handley, “From Protocol Stack to Protocol Heap - Role-Based Architecture,” *ACM SIGCOMM Computer Communication Review (CCR)*, vol. 33, no. 1, pp. 17–22, January 2003.
- [13] C. Tschudin, “Flexible Protocol Stacks,” in *Proc. of ACM SIGCOMM '91*, Zürich, Switzerland, September 1991, pp. 197–205.
- [14] R. Kumar, S. Pal-Chaudhuri, D. Johnson, and U. Ramachandran, “Network Stack Architecture for Future Sensors,” Rice Computer Science, Tech. Rep. TR-04-447, 2004.
- [15] M. S. Corson and J. Macker, “Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations,” IETF, RFC 2501, January 1999.
- [16] B. Krishnamachari, D. Estrin, and S. Wicker, “Modelling Data-Centric Routing in Wireless Sensor Networks,” University of Southern California, Tech. Rep. CENG 02-14, 2002.
- [17] L. Wischhof, A. Ebner, H. Rohling, M. Lott, and R. Halfmann, “SOTIS - A Self-Organizing Traffic Information System,” in *Proc. of IEEE VTC Spring '03*, Jeju, Korea, April 2003.
- [18] M. Torrent-Moreno, D. Jiang, and H. Hartenstein, “Broadcast Reception Rates and Effects of Priority Access in 802.11-Based Vehicular Ad-Hoc Networks,” in *Proc. of ACM VANET '04*, Philadelphia, PA, October 2004, pp. 10–18.