A Tutorial Survey on Vehicular Ad Hoc Networks

Hannes Hartenstein, University of Karlsruhe
Kenneth P. Laberteaux, Toyota Technical Center

ABSTRACT

There has been significant interest and progress in the field of vehicular ad hoc networks over the last several years. VANETs comprise vehicle-to-vehicle and vehicle-to-infrastructure communications based on wireless local area network technologies. The dinstinctive set of candidate applications (e.g., collision warning and local traffic information for drivers), resources (licensed spectrum, rechargeable power source), and the environment (e.g., vehicular traffic flow patterns, privacy concerns) make the VANET a unique area of wireless communication. This article gives an overview of the field, providing motivations, challenges, and a snapshot of proposed solutions.

INTRODUCTION

The concept of leveraging wireless communication in vehicles has fascinated researchers since the 1980s [1]. In the last few years, we have witnessed a large increase in research and development in this area. Several factors have led to this development, including the wide adoption (and subsequent drop in cost) of IEEE 802.11 technologies; the embrace of vehicle manufactures of information technology to address the safety, environmental, and comfort issues of their vehicles; and the commitment of large national and regional governments to allocate wireless spectrum for vehicular wireless communication. Although cellular networks enable convenient voice communication and simple infotainment services to drivers and passengers, they are not well-suited for certain direct vehicle-to-vehicle or vehicle-to-infrastructure communications. However, vehicular ad hoc networks (VANETs), which offer direct communication between vehicles and to and from roadside units (RSUs), can send and receive hazard warnings or information on the current traffic situation with minimal latency.

With the availability since the late 1990s of low-cost, global-positioning system (GPS) receivers and wireless local area network (WLAN) transceivers, research in the field of inter-vehicular communication gained considerable momentum (e.g., [2]). The major goals of these activities are to increase road safety and transportation efficiency, as well as to reduce the impact of transportation on the environment. These three classes of applications of VANET technology are not completely orthogonal: for example, reducing the number of accidents can in turn reduce the number of traffic jams, which could reduce the level of environmental impact (Fig. 1). Due to the importance of these goals for both the individual and the nation, various projects are underway, or recently were completed, and several consortia were set up to explore the potential of VANETs (Fig. 2). These consortia projects involve several constituencies, including the automotive industry, the road operators, tolling agencies, and other service providers. These projects are funded substantially by national governments. National governments also contribute licensed spectrum, generally in the 5.8/5.9-GHz band and at least in Japan, the 700-MHz band.

The term VANET was originally adopted to reflect the *ad hoc* nature of these highly dynamic networks. However, because the term *ad hoc network* was associated widely with unicast routing-related research, there is currently a debate among the pioneers of this field about redefining the acronym VANET to deemphasize ad hoc networking. Because this discussion has not yet reached consensus, we will continue to refer to vehicle-to-vehicle and vehicle-to-roadside communication based on wireless local area networking technology as a VANET.

In this article we present a tutorial overview[1] on the communication and networking aspects of vehicular ad hoc networks. We first look more closely at the potential applications and their requirements with respect to the communication platform. Then, we present what we consider the specific challenges of VANET design. Because cost and safety dictate that simulations are a necessary tool for doing research in this field, we continue with a brief introduction to vehicular traffic flow models and some radio channel basics required for realistic assessments of VANET systems and protocols. After the sections on challenges and tools, we concentrate on the assets to meet the challenges: we look at the IEEE 802.11p draft [3], the IEEE 1609 Wireless Access in Vehicular Environments (WAVE) trial

[1] *This article is based on a tutorial on VANETs we presented at ACM MobiCom/MobiHoc 2007 in Montreal, Canada.*

0163-6804/08/$25.00 © 2008 IEEE

use standards [4], rate and power control, position-based forwarding and information dissemination approaches, and appropriate middleware. We also address security and privacy issues in VANETs, because these are critical to system dependability and customer acceptance. Finally, we summarize the current state-of-the-art and discuss important open issues.

VANET Applications and their Requirements

Extensive lists of potential applications were compiled and assessed by the various projects and consortia. Typically, applications are categorized as safety, transport efficiency, and information/entertainment applications. Examples for each category are:

- Cooperative forward collision warning, namely, to avoid rear-end collisions
- Traffic light optimal speed advisory, namely, to assist the driver to arrive during a *green phase*
- Remote wireless diagnosis, namely, to make the state of the vehicle accessible for remote diagnosis

To evaluate the chances of success, applications were analyzed as to whether their requirements can be satisfied and whether (and to what degree) they will provide a beneficial impact. On the requirements side, a prominent factor is the required penetration rate (i.e., the percentage of vehicles equipped with VANET technology compared to the vehicle population) to enable acceptable operation of the application. Technical requirements define packet sizes, required frequency or accuracy of updated information, communication ranges, latency constraints, security levels, and required infrastructure. On the added-value side, applications are assessed with respect to the level they increase safety or transport efficiency or serve desirable information requirements. Quantitative evaluations of added value are tricky because human factors come into play: for example, accurate prognoses of road traffic proved to be an extremely hard task because those prognoses must take into account the *feedback loop* — how humans react on these prognoses.

For safety-related applications, the Vehicle Safety Communications (VSC) consortium identified eight high potential applications [5]: traffic signal violation warning, curve speed warning, emergency electronic brake light, pre-crash sensing, cooperative forward collision warning, left turn assistant, lane-change warning, and stop sign movement assistant. Note that four of these applications require vehicle-to-vehicle communication, whereas the other four require communication with roadside infrastructure. The derived technical requirements show the importance of one-hop broadcast communication (i.e., a vehicle simply transmits a packet, and every vehicle that is able to receive it directly is considered a one-hop neighbor), which comes in two flavors: event-driven and periodic. Event-driven messages are sent when a hazardous situation is detected. Periodic messages proactively inform neighboring vehicles about status, for example,

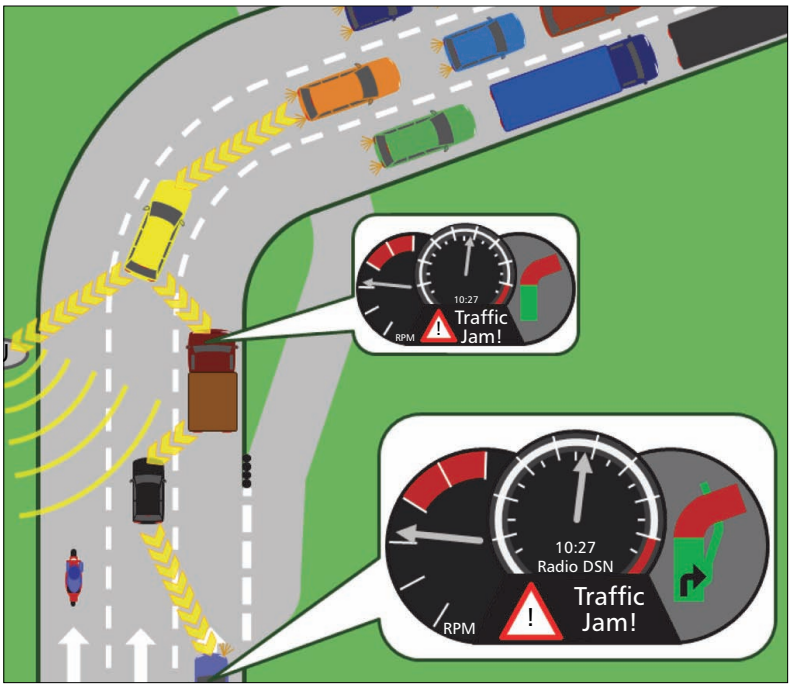

Figure 1. *By vehicle-to-vehicle and vehicle-to-roadside communication, accidents can be avoided (e.g., by not colliding with a traffic jam) and traffic efficiency can be increased (e.g., by taking alternative routes).*

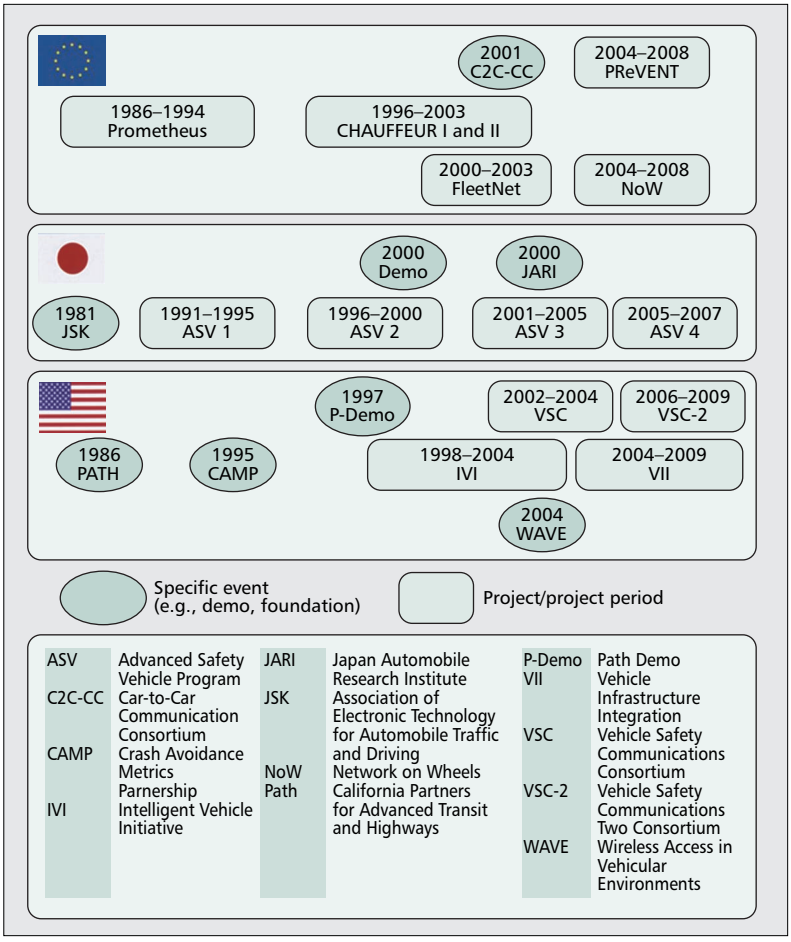

Figure 2. *A nonexhaustive overview of pioneering activities and milestones that show the evolution of the topic of VANET research around the globe. In addition to that, various projects are currently funded in the EU, Japan, the United States, and other parts of the world.*

A central challenge of VANETs is that no communication coordinator can be assumed. Although some applications likely will involve infrastructure, several applications will be expected to function reliably using decentralized communications.

the position of the sending vehicle. The VSC suggests that periodic one-hop broadcasts that are required, for example, with forward collision warning, require a frequency of 10 messages per second, with a maximum latency of 100 ms and a minimum range of 150 meters. In the meantime, studies show that in dense vehicular traffic scenarios, these periodic messages can overload the available radio channel. Thus, adaptive transmit power and rate control mechanisms are required as discussed below.

For transportation efficiency applications, the Car-to-Car Communication Consortium (C2C-CC) [6] analyzed exemplarily enhanced route guidance and navigation, green light optimal speed advisory, and lane merging assistants. Whereas for the first two applications, roadside infrastructure is considered a prerequisite, the lane merging assistant is assumed to be based on vehicle-to-vehicle communication. The C2C-CC particularly emphasizes the importance of a reasonable level of security to establish the required trust of the obtained information.

Ideas for information and entertainment applications consist of quite a diverse set: tolling (one of the initial motivators for vehicle-to-infrastructure communications), point-of-interest notifications, fuel consumption management, podcasting, and multihop wireless Internet access, to name a few. Due to this diversity, a requirements-benefits analysis must be done on a case-by-case basis. An important consideration for all information/entertainment applications is whether the application is ideally implemented using the same communication platform as used by traffic safety and efficiency applications or whether they could be better implemented using competing/separate network technologies.

Main Challenges of VANETs

Technical Challenges

A central challenge of VANETs is that no communication coordinator can be assumed. Although some applications likely will involve infrastructure (e.g., traffic signal violation warning, toll collection), several applications will be expected to function reliably using decentralized communications. Because no central coordination or handshaking protocol can be assumed, and given that many applications will be broadcasting information of interest to many surrounding cars, the necessity of a single, shared control channel can be derived (even when multiple channels are available using one or more transceivers, at least one shared control channel is required). This one-channel paradigm, together with the requirement for distributed control, leads to some of the key challenges of VANET design. The very well-known problem of hidden and exposed terminals is problematic. Clearly, medium access control (MAC) is a key issue in the design of VANETs. Although time division multiple access (TDMA)- and spatial division multiple access (SDMA)-based approaches were proposed, the main focus today is on using the IEEE 802.11 carrier sense multiple access (CSMA)-based MAC for VANETs. This is due to availability and cost considerations and accepts the random elements of such a MAC. The bandwidth of the frequency channels currently assigned or foreseen for VANET applications ranges from 10 to 20 MHz. With a high vehicular traffic density, those channels easily could suffer from channel congestion. Making use of more than one channel leads to multichannel synchronization problems, in particular for the case of a single transceiver per vehicle and to co-channel interference problems.

Other challenges are the dynamic network topology based on the mobility of the vehicles and the environmental impact on the radio propagation. The latter must take into account that the low antenna heights and the attenuation/reflection of all the moving metal vehicle bodies provides for adverse radio channel conditions. All together, VANETs must work properly in a wide range of conditions, including sparse and dense vehicular traffic. There is a strong need for adaptive transmit power and rate control to achieve a reasonable degree of reliable and low latency communication.

In addition, there is a challenge in balancing security and privacy needs. On the one hand, the receivers want to make sure that they can trust the source of information. On the other hand, the availability of such trust might contradict the privacy requirements of a sender.

Socio-Economic Challenges

Market introduction of direct communication between vehicles is suffering from the network effect: the added value for one customer depends on the number of customers in total who have equipped their vehicle with VANET technology. A key question, therefore, is how to convince early-adopters to buy VANET equipment for their vehicles. Many options have been discussed, ranging from enforcement by law, preferred insurance premiums, and attractive deployment applications. In general, it seems likely that some installed roadside infrastructure will be used to lure the very first customers. As Pravin Varayia put it in his ACM VANET 2005 keynote address, by analyzing the cost-benefit gap, one can argue that reception of high value safety messages with almost zero probability (during the market introduction period) might be of smaller value than receiving non-safety announcements available from day one. Still, with respect to the infrastructure on the roadside, backhaul connectivity and IT-management issues arise that might affect many parties (various communities, road operators, etc.), a fact that led to troublesome experiences for those who have tried to set up real-world field tests.

Essential Topology and Channel Features and Models

To understand the specific challenges of VANETs compared to other mobile wireless networks and to perform simulations, models capturing the essential features of vehicular traffic flows and of radio channel performance are of fundamental importance.

The design and analysis of realistic vehicular traffic flow models has been pursued for more

than five decades [7]. For VANET simulations, *microscopic* models are typically required because they provide space-time behavior of vehicles (and drivers) and their interactions on an individual level. However, it is equally important to match the *macroscopic* features of real traffic, namely, features such as the average number of vehicles per hour passing a specific cross-section, the average number of vehicles per kilometer, or the headway that specifies the difference in passage times of two successive vehicles.

Among the classical microscopic models, the car-following model by Wiedemann, which is based on a psycho-physical model that considers the human driver's perception and reaction and the Nagel-Schreckenberg model, which is based on a cellular automaton approach, are widely used and cited. The Wiedemann model, with its many extensions, is considered a high-fidelity model. The Nagel-Schreckenberg model is typically seen as a low-fidelity model. Here, low-fidelity implies the sacrifice of some degree of realism with respect to vehicle acceleration/deceleration to gain simulation speed and scalability. For VANET research, the required level of accuracy is not clear yet.

For vehicular traffic flow simulations, several tools are available. Most notably, there are various commercial traffic simulation products available like VISSIM, AIMSUN, and Paramics. The Federal Highway Administration (USA), which previously funded CORSIM, is currently funding model research and standardization for existing simulators within their next-generation simulation (NGSIM) program.

From the research community proposals like SHIFT, STRAW, and VanetMobiSim were made available to facilitate accessibility for networking studies (see, e.g., [8] for a survey on mobility models for VANET research). For VANET research, the vehicular traffic flow simulators either produce trace files that are given as input to a network simulator, or the traffic flow simulator must be coupled with the network simulator to allow feedback from communication to vehicular traffic behavior (e.g., [9]). In this context, there are at least three challenges that must be addressed by the research community:

- Specifications of APIs for coupling traffic flow and networking simulators
- Modeling how drivers react to the additional information provided by VANETs
- Benchmark definitions to make simulation studies and results comparable

In addition, for safety-related studies, accident models would be required because current traffic flow simulators typically do not produce accidents.

The second important building block for accurate VANET simulations is given by models for the radio channel and for the packet reception capabilities of the receiving interface. Real-world measurements show that deterministic radio propagation models should be avoided because they do not capture the probabilistic effects of small scale fading that have a significant impact on packet reception. The Nakagami-m distribution was proposed and used to cover a wide range of potential channel conditions [2].

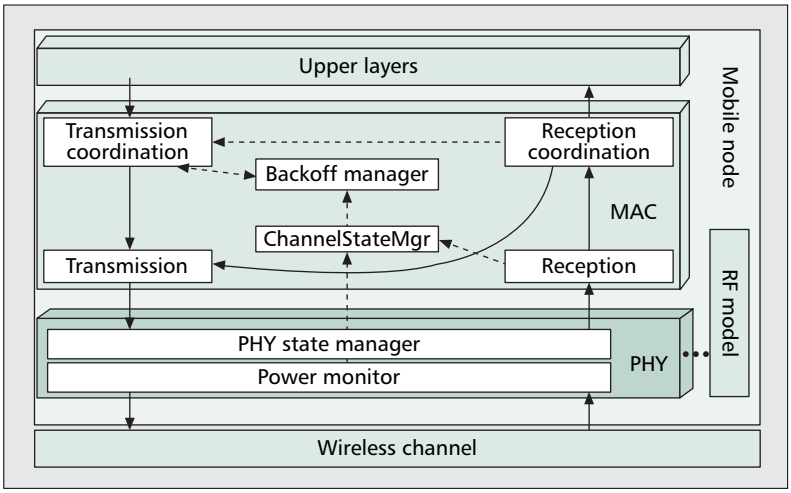

Figure 3. *Architecture of the overhaul of the IEEE 802.11 implementation in the network simulator NS-2.33 [10].*

Of course, some environmental factors (e.g., weather, surrounding buildings, or traffic) are difficult to capture and often ignored in simulation. However, protocols can be checked over a wide range of channel parameters to understand their sensitivity with respect to those parameters.

Although channel conditions can be challenging, improved receiver capabilities might help to decode packets. Modern chipsets are able to capture packets almost independently of the order of their arrival. Often, network simulators only provide less powerful capturing capabilities that do not correspond to modern chipsets. Capture is a highly important capability for dealing with the one-channel problem as outlined above; thus, accurately modeling the capture capability is essential for producing credible results. Mercedes-Benz Research & Development North America and the University of Karlsruhe developed a new physical (PHY) and MAC module [10][2] for the network simulator NS-2. The module comprises an implementation of the Nakagami-m distribution as channel model, accurate capture modeling, and the IEEE 802.11a/p standard draft in a clean software architecture (Fig. 3) that is composed of separate building blocks for radio frequency (RF) model, PHY, and MAC elements. Still, modeling and analyzing the effect of large scale fading, in particular of moving radio-wave obstacles like a truck between two cars, requires more attention from the communications community.

Protocols, Architectures, and Standards

As mentioned above, the current focus for the PHY/MAC layers is based on IEEE 802.11 with distributed coordination function (DCF). Of course, guaranteed quality of service support cannot be given with such a system. The ASTM (originally, the American Society for Testing and Materials) modified the 802.11a standard to better match the vehicular environment. Based on this effort, IEEE is currently standardizing the corresponding 802.11p standard. IEEE 802.11p

[2] *Included in release NS-2.33.*

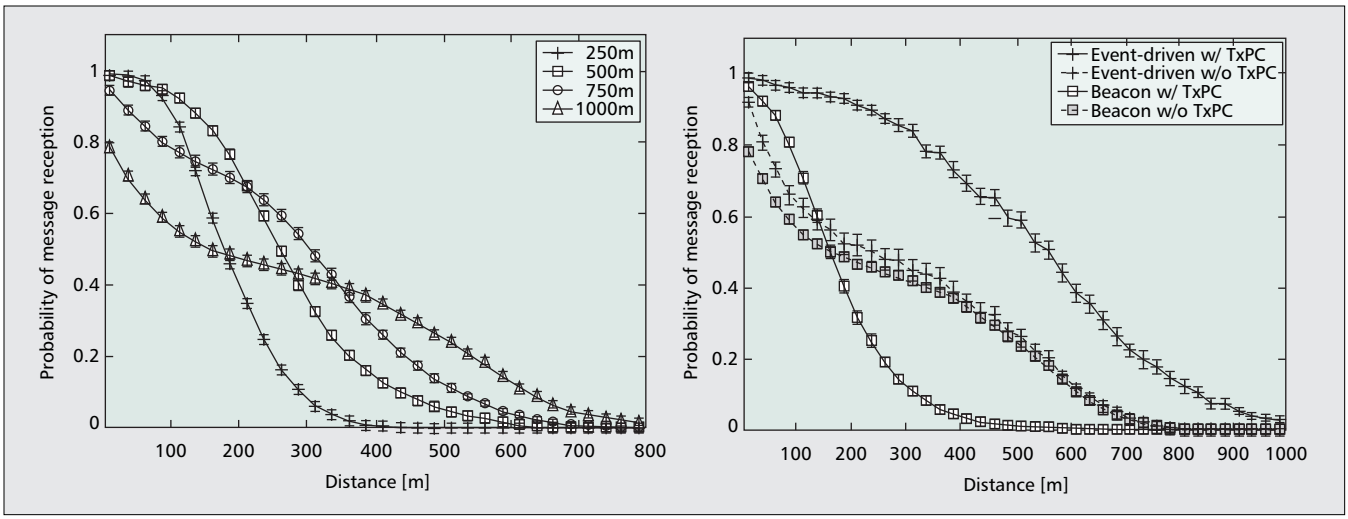

Figure 4. *The graphs show the probability of message reception depending on the distance to the sender for one-hop broadcast communication. By increasing transmit power in order to reach larger distances (250–1000 m), one combats fading but increases channel saturation, which leads to unacceptable reception rates close to the sender (left); controlling the beacon load on the channel with a distributed transmit power control (TxPC), the event-driven messages will be successfully received with a higher probability while the beacon message reception rate is increased where the beacons are important (i.e., close to the sender; right) [11].*

is based on an orthogonal frequency-division multiplexing (OFDM) PHY layer but uses 10-MHz channels as opposed to the 20-MHz channels for IEEE 802.11a. As a result, data rates ranges from 3 to 27 Mb/s for each channel, where lower rates are often preferred in order to obtain robust communication. IEEE 802.11a and 11p operate in the 5.8/5.9-GHz band.

Because the basic type of communication in a VANET is based on one-hop broadcasts, the IEEE 802.11 MAC boils down to a simple CSMA scheme. However, many parameters can influence the probability of packet reception. A partial list includes vehicular traffic density, radio channel conditions, data rate, transmit power, contention window sizes, and the prioritization of packets.

For prioritization, the ideas of enhanced distributed channel access (EDCA), formerly described in IEEE 802.11e and now part of 802.11-2007, can be used, and configuration values are proposed in IEEE 1609.4. Four access categories with independent channel access queues are provided by adjusting the arbitration interframe space and the contention window size.

A comprehensive simulation study of the effects of parameters on the probability of reception is presented in [11]. The study shows that for a more saturated channel, it is preferable to use a data rate of 3 Mb/s instead of higher data rates due to the lower capture threshold. Also, the prioritized channel access based on IEEE 802.11e can be shown to lead to improved channel access times and higher probability of reception for those packets that receive a higher priority. In total, however, the results show that out-of-the-box IEEE 802.11p alone is not sufficient to provide an appropriate level of quality of service to support traffic safety-related applications. For example, as illustrated in Fig. 4, for a more saturated radio channel, increasing the transmit power successfully combats fading, but it comes at the price of also increasing saturation, which leads to more packet collisions close to the sender of a packet. Therefore, it is suggested that IEEE 802.11p be combined with adaptive transmit power and rate control to avoid channel congestion. Figure 4 also shows the potential of a distributed transmit power control approach [11] for the differentiation of traffic classes (like periodic beacon messages and event-driven warnings). The periodic beacon messages that are used to proactively indicate the current status of a vehicle to all neighboring vehicles are sent out as one-hop broadcast messages up to 10 times per second. Because those beacons should have a high probability of reception close to the sender but are usually less important for greater distances, transmit power control can be used successfully to limit the beaconing load on the channel. By limiting the beaconing load, one can ensure that high priority, low-bandwidth traffic, like emergency warnings, can be received with a high probability for a wide range of distances to the sender. Underlying the simulation results shown in Fig. 4 is a Nakagami-m radio propagation model with m set to three and a highway segment with 66 vehicles per kilometer. Analogous results for determining the optimal packet rate are presented in [12]. Joint optimal transmit and power control is still an open issue.

The results given in Fig. 4 are based only on one-hop broadcast communication. Of course, multihop information dissemination is also of interest, for example, to enable drivers to make smart driving decisions well ahead of time. Since several VANET applications are strongly dependant on the geographic location of a vehicle, positional information is of crucial importance. This information also can be used for forwarding decisions of packets. Proposals have been made either based on classical position-based forwarding or based on contention-based forwarding (CBF). Contention-based forwarding is based on

an implicit or opportunistic forwarder selection, where all receivers of a one-hop broadcast contend for the right to retransmit the packet. The contention criterion could be based, for example, on the position of a node with respect to the desired destination position. A node closer to the destination would start a retransmission attempt after a shorter time period than a node farther away from the destination. After one forwarder "wins" the contention and transmits, the other potential forwarders — that observe the transmission of the "winning" node — cease their efforts to forward that packet. Thus, with CBF, the next-hop selection is not based on some logical neighbor information but on the physical "as is" situation, thereby providing a high degree of robustness to network and environmental dynamics.

Information dissemination in VANETs deals with both safety and non-safety-related information dissemination; for example, see [9]. Scalability is a key issue for information dissemination to avoid a *broadcast storm*. Scalable aggregation mechanisms were proposed that borrow ideas from peer-to-peer networks. To ensure that vehicles *understand* the messages independent of their makes and brands, message sets as defined in the SAE J2735 Dedicated Short Range Communications Message Set Dictionary (December 2006) were proposed to exchange vehicle status and warning information in a standardized way. In addition, these messages can be optimized by considering the low entropy often present in vehicle location histories; namely, the rate and size of messages can be reduced if appropriate predictive methods are used for the location and speed of a vehicle [13].

From a system and protocol stack point of view, two questions arise:

- How can all the above elements be brought together?
- What other aspects must be considered for implementation?

On the one hand, the vehicular network could simply be an extension of the Internet, leveraging the same User Datagram Protocol/Internet Protocol (UDP/IP)-based methods. On the other hand, there is a strong need for supporting VANET-centric applications, for example, traffic safety and efficiency. As argued above, such vehicle-centric applications ideally control and access PHY and MAC parameters. Therefore, a dual stack architecture was proposed in the IEEE 1609 WAVE trial-use standard (Fig. 5). The IEEE 1609 framework builds on IEEE 802.11p as PHY/MAC and provides two parallel stacks on top of it, one for UDP/Transmission Control Protocol (TCP) over IPv6 and one called Wave Short Message Protocol (WSMP). With WSMP, various low level parameters can be specified like data rate and transmit power level.

The complete IEEE 1609 framework currently consists of four parts, which specify the networking services (1609.3), multi-channel operation (1609.4), security issues (1609.2), and a specific transponder-like application called resource manager (1609.1). In particular, the multichannel operation has drawn considerable attention because the challenge of using several channels, for example, as assigned in the United States by the Federal Communications Commission, with only one transceiver, does not yet have a simple and efficient solution. To understand this, consider that one must guarantee that all vehicles monitor the control channel at given intervals during which safety messages are exchanged. Therefore, tight time synchronization among the vehicles would be required. Vehicles would then switch between service channels and the control channel for fixed time slots. Clearly, such a channel-switching approach does not make the most efficient use of the allocated frequency channels.

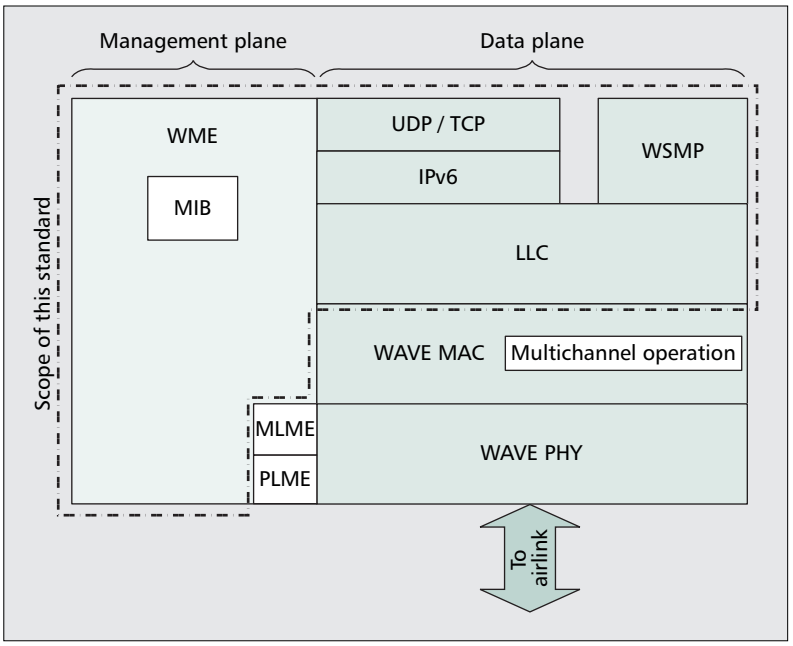

Figure 5. *The protocol stack as suggested by the IEEE 1609 family of standards for wireless access in vehicular environments [4].*

Time will tell how successful the current standardization activities will be. A big challenge, however, is the problem of optimally adjusting the many communication/networking parameters to match the goals of the respective applications in a context-aware fashion. For optimal control, mathematical models covering the essential relationships between vehicular density, transmit power, data rate, and the resulting probability of reception are still required.

Security and Privacy

The efficacy and reliability of a system where information is gathered and shared among autonomous entities raises concerns about data authenticity. For example, a sender could misrepresent observations to gain advantage (e.g., a vehicle V falsely reports that its desired road R is jammed with traffic, thereby encouraging others to avoid R and providing a less-congested trip for V on R). More malicious reporters could impersonate other vehicles or road-side infrastructure to trigger safety hazards. Vehicles could reduce this threat by creating networks of trust and ignoring, or at least distrusting, information from untrusted senders.

A trusted communication generally requires that two properties are met:

Other policy issues remain, such as management and cost of a trusted certificate authority. In addition, a process should be established to determine when a specific certificate should be revoked due to evidence of malfunction or tampering.

- The sender is conclusively accepted as a trusted source.
- While in transit, the contents of the sender's message are not tampered with.

An overview of VANET security can be found in [14]. Various consortia presently are addressing VANET security and privacy issues, including the Crash Avoidance Metrics Partnership (CAMP) Vehicle Safety Communications-Applications project, the Vehicle Infrastructure Integration (VII) project, the SeVeCom project, the Embedded Security for Cars (ESCAR) Conference, and others. The trial-use standard IEEE 1609.2 (previously named P1556) also addresses security services for VANETs.

A key challenge of securing VANETs is to provide sender authentication in broadcast communication scenarios. This so-called broadcast authentication is challenging because vehicles might not have met before, and link-layer losses might affect different broadcast receivers with differing severity.

Conventional Digital Signatures

Broadcast authentication is typically achieved through the use of public key signatures. To ensure that the public key belongs to the node being authenticated, a structure called a public key infrastructure (PKI) typically is required. In a PKI, certificate authorities (CAs) sign bindings between public keys and node identifiers; these bindings are called *certificates*. Then, any entity that trusts this CA will store its public key. In the current IEEE 1609.2 proposal, messages are authenticated using the Elliptic Curve Digital Signature Algorithm (ECDSA) scheme. Each message also includes a certificate, which with ECDSA can be no smaller than 60 bytes. Note that to economize over-the-air bandwidth, it is possible for verifiers to cache the certificates and public keys of a signer. This might allow the signer to send certificates in a subset of data messages or in separate certificate-sharing messages.

In addition to the bandwidth overhead, there are additional concerns about the draft IEEE 1609.2. For one, the hardware costs involved with verifying a digital signature for every incoming message (e.g., possibly 2500 messages/sec) could be very expensive. In addition, privacy concerns are not fully addressed.

Lightweight Broadcast Authentication

The large computational burden (i.e., the hardware cost) of verifying a digital signature for every received packet has led to an exploration for alternatives. Recently, timed efficient stream loss-tolerant authentication (TESLA) was proposed [15]. Briefly stated, in TESLA, the sender signs messages using a symmetric signature algorithm and then broadcasts this message with the signature (but importantly, not the key). A short time later, the sender broadcasts the key and instructs all that this disclosed key is not to be used in the future. Receivers cache the original message until the key is received and then verify the signature. Because this verification uses symmetric cryptographic primitives, it requires approximately 1000 times less computational resources than ECDSA. Full details of this proposal can be found in [16].

Privacy and Other Issues

There is tension between the receiver's goal of strong message authentication and the sender's goal of strong privacy [16]. Several candidate solutions are under consideration, including the use of multiple pseudo-identifiers per vehicle. In [17], various additional ideas to mitigate unauthorized tracking such as random silent periods, hiding in groups, or the use of power control are discussed and assessed. However, a purely technical solution may not be sufficient. Consumer acceptance may be reduced if police issue speeding tickets based on vehicle-originating safety messages. Other policy issues remain, such as management and cost of a trusted certificate authority. In addition, a process should be established to determine when a specific certificate should be revoked due to evidence of malfunction or tampering.

Conclusion and Future Perspectives

To summarize the state of VANETs — the feasibility of direct and wireless multihop vehicle-to-vehicle and vehicle-to-infrastructure communication based on wireless local area networking technologies was proven, and essential building blocks exist today. Those building blocks are provided by the IEEE 802.11p draft, by the IEEE 1609 WAVE framework, by proposals for rate and power control to avoid channel congestion, and by approaches for information dissemination. In addition, message sets to achieve harmonization on a semantic level have been standardized, the security requirements have been analyzed in detail, and simulation methodology for VANET research has greatly improved.

Still, there are several challenges ahead. First of all, the *beneficial* impact of VANETs on traffic safety and efficiency must be shown. As with the introduction of anti-locking brakes, it is not clear *per se* that simply introducing VANETs will automatically and monotonically increase safety and efficiency. To gain a better understanding of real-world VANETs, field operational tests are underway all over the world. In addition, with those real-world experiments, simulation models can be refined, platforms can be further developed, and IT management issues can be investigated more deeply. In particular, the Vehicle Infrastructure Integration project and similar activities could highly influence the evolution of VANETs in the coming years.

To show the impact of VANETs on traffic safety and efficiency via simulations, accident and human behavior models are required, that is, one must understand how drivers will react based on the additional information provided by VANETs. With respect to simulation methodology, a set of standardized benchmarks and test scenarios would be useful to make protocol and model proposals comparable with each other. As currently discussed in the field of grid computing, VANET research and standardization would benefit from improved

provenance management for simulation models and results.

A key task for the future is to properly specify the communication requirements of VANET applications and to derive the corresponding optimal tuning of parameters of the communication system, taking into account the current channel and traffic situation. Clearly, the availability of mathematical models describing, for example, probability of reception or latency or packets depending on vehicular and data traffic load would greatly help such an effort [18]. Still, even with mathematical models and optimal parameter tunings available, the "true" channel load conditions must be correctly estimated.

Finally, there are many other challenges that will have a strong influence on the future of VANETs. First of all, there are many players in the game struggling to agree, particularly on the topic of who must pay. The market introduction challenge is, of course, related to this issue. Second, a VANET system must work reliably in any situation or should be able to detect those situations in which it is not working reliably. Thus, roll-out will strongly depend on the level of maturity gained over the coming years.

A VANET system must work reliably in any situation or should be able to detect those situations in which it is not working reliably. Thus, roll-out will strongly depend on the level of maturity gained over the coming years.

ACKNOWLEDGMENTS

We wish to thank the anonymous reviewers for their constructive comments that greatly improved the article. In addition, we would like to thank J. Härri, T. Höllrigl, M. Killat, F. Schmidt-Eisenlohr, and M. Torrent-Moreno for their insightful comments and help in preparing this article.

REFERENCES

[1] H. Kawashima, "Japanese Perspective of Driver Information Systems," *Transportation*, vol. 17, no. 3, Sept. 1990, pp. 263–84.
[2] D. Jiang *et al.*, "Design of 5.9 GHz DSRC-based Vehicular Safety Communication," *IEEE Wireless Commun.*, vol. 13, no. 5, Oct. 2006, pp. 36–43.
[3] IEEE 802.11p Amendment, "Wireless Access in Vehicular Environments," v. D3.0, 2007, work in progress.
[4] IEEE 1609 Family of Standards for Wireless Access in Vehicular Environments; available from IEEE Standards.
[5] Vehicle Safety Communications Project, Final Report, DOT HS 810 591, April 2006.
[6] Manifesto of the Car-to-Car Communication Consortium; www.car-to-car.org, Sept. 2007.
[7] S. P. Hoogendoorn and P. H. L. Bovy, "State-of-the-Art of Vehicular Traffic Flow Modeling," *J. Sys. and Control Eng.*, vol. 215, no. 4, Aug. 2001, pp. 283–304.
[8] J. Härri, F. Filali, and C. Bonnet, "Mobility Models for Vehicular Ad Hoc Networks: A Survey and Taxonomy," research rep. RR-06-168, Institut Eurecom, Mar. 2007.
[9] M. Caliskan, D. Graupner, and M. Mauve, "Decentralized Discovery of Free Parking Places," *Proc. 3rd ACM Int'l. Wksp. Vehic. Ad Hoc Networks*, Los Angeles, CA, Sept. 2006, pp. 30–39.
[10] Q. Chen *et al.*, "Overhaul of IEEE 802.11 Modeling and Simulation Architecture in NS-2," *Proc. 10th ACM/IEEE Int'l. Symp. Modeling, Analysis, and Simulation of Wireless and Mobile Sys.*, Chania, Greece, Oct. 2007, pp. 159–68.
[11] M. Torrent-Moreno, "Inter-Vehicle Communications: Achieving Safety in a Distributed Wireless Environment — Challenges, Systems and Protocols," diss., Univ. of Karlsruhe, July 2007; http://dsn.tm.uni-karlsruhe.de.
[12] Q. Xu *et al.*, "Medium Access Control Protocol Design for Vehicle-Vehicle Safety Messages," *IEEE Trans. Vehic. Tech.*, vol. 56, no. 2, Mar. 2007, pp. 499–518.
[13] C. L. Robinson *et al.*, "Efficient Message Composition and Coding for Cooperative Vehicular Safety Applications," *IEEE Trans. Vehic. Tech.*, vol. 56, no. 6, Nov. 2007, pp. 3244–55.
[14] M. Raya, P. Papadimitratos, and J.-P. Hubaux, "Securing Vehicular Communications," *IEEE Wireless Commun.*, Special Issue on Inter-Vehicular Commun., vol. 13, no. 5, Oct. 2006, pp. 8–15.
[15] A. Perrig et al., "The TESLA Broadcast Authentication Protocol," *CryptoBytes*, vol. 5, no. 2, Summer–Fall 2002, pp. 2–13.
[16] Y.-C. Hu and K. Laberteaux, "Strong Security on a Budget," Wksp. Embedded Security for Cars, Nov. 2006; http://www.crhc.uiuc.edu/~yihchun/
[17] K. Sampigethaya *et al.*, "AMOEBA: Robust Location Privacy Scheme for VANET," *IEEE JSAC*, vol. 25, no. 8, Oct. 2007, pp. 1569–89.
[18] M. Killat *et al.*, "Enabling Efficient and Accurate Large-Scale Simulations of VANETs for Vehicular Traffic Management," *Proc. 4th ACM Int'l. Wksp. Vehic. Ad Hoc Networks*, Montreal, Canada, Sept. 2007, pp. 29–38.

BIOGRAPHIES

HANNES HARTENSTEIN (hannes.hartenstein@kit.edu) holds a diploma in mathematics and a doctoral degree in computer science, both from Albert-Ludwigs-Universität, Freiburg, Germany. He is a full professor for decentralized systems and network services at the Karlsruhe Institute of Technology (KIT), Germany, which was formed by the University of Karlsruhe and the Research Center Karlsruhe. His research interests include inter-vehicle communications, peer-to-peer networks, sensor networks, and IT management. Prior to joining the University of Karlsruhe, he was a senior research staff member with NEC Europe. He was NEC's project leader (2001–2003) for the FleetNet — Internet on the Road project, partly funded by the German Ministry of Education and Research (BMBF) and is now involved in the NOW: Network on Wheels project. He has been TPC co-chair and general chair of various respected ACM and IEEE international workshops and symposia on vehicular communications.

KENNETH P. LABERTEAUX received his B.S.E. (summa cum laude) in electrical engineering from the University of Michigan, Ann Arbor, in 1992. He received his M.S. (1996) and Ph.D. (2000) degrees in electrical engineering from the University of Notre Dame, focusing on adaptive control for communications. He is a senior principal research engineer for the Toyota Technical Center, Ann Arbor, Michigan. His research focus is information-rich vehicular safety systems; focusing on architecture, security, and protocol design for vehicle-to-vehicle and vehicle-to-roadside wireless communication. He was a founder and two-year (2004, 2005) general co-chair of the highly selective international Vehicular Ad Hoc Networks (VANET) workshop. He serves as the architect and technical lead for communications research within a multiyear multimillion-dollar Vehicle Safety Communications-Applications collaboration project between the U.S. government and several automotive companies.