3RD QUARTER 2008, VOLUME 10, NO. 3

IEEE COMMUNICATIONS SURVEYS

www.comsoc.org/pubs/surveys

VEHICLE AD HOC NETWORKS: APPLICATIONS AND RELATED TECHNICAL ISSUES

YASSER TOOR AND PAUL MÜHLETHALER, INRIA
ANIS LAOUITI, GET/INT
ARNAUD DE LA FORTELLE, ECOLE DES MINES

ABSTRACT

This article presents a comprehensive survey of the state-of-the-art for vehicle ad hoc networks. We start by reviewing the possible applications that can be used in VANETs, namely, safety and user applications, and by identifying their requirements. Then, we classify the solutions proposed in the literature according to their location in the open system interconnection reference model and their relationship to safety or user applications. We analyze their advantages and shortcomings and provide our suggestions for a better approach. We also describe the different methods used to simulate and evaluate the proposed solutions. Finally, we conclude with suggestions for a general architecture that can form the basis for a practical VANET.

Improving road safety is a subject of intense interest and research. One possible way of preventing accidents is by using safety applications that communicate through wireless networks. Also, as more and more people afford cars, the demand for in-vehicle entertainment is increasing. With the recent developments in computing and wireless communication technologies, networks that can form the basis for such applications can be envisioned. The networks will be completely mobile, require little or no infrastructure, and support the applications in a dynamic, random, and multihop topology. These mobile ad hoc networks (MANETs) have several characteristics [1], such as dynamic topologies, limited bandwidth, limited energy, and so on. Because a MANET is an autonomous network, the mobile nodes can be located on airplanes, ships, trucks, or cars. Hence, vehicle ad hoc networks (VANETs) are a special case of mobile ad hoc networks. They can be formed between vehicles with vehicle to vehicle (V2V) communication or between vehicles and an infrastructure with vehicle to infrastructure (V2I) communication, as shown in Fig. 1. These VANETs can provide the basis for improving road safety as acknowledged in numerous projects working toward this goal [2–4].

VANETs have several properties that distinguish them from other MANETs. Nodes (vehicles) in VANETs are highly mobile; the probability of network partitions is higher, and end-to-end connectivity is not guaranteed but rather is a luxury [5]. However, although VANETs do have dynamic topologies, they are not completely random. The movement of nodes in a VANET is relatively predictable because it is restricted to the roads on which the vehicles travel. This has several advantages and disadvantages for applications and routing protocols. The predictability of the position of a vehicle allows an improvement in link selection, but the linear topology of VANETs reduces the possible path redundancy. The bandwidth issue also is exacerbated due to intersections, traffic jams, and the presence of buildings beside the roads, especially in an urban environment. VANETs also have the potential to grow to a very large scale. For example, consider a section of a road with three lanes. In normal conditions, with an inter-vehicle distance of 70 m,[1] we have around 70 vehicles within a radius of 1 km around a given car. During a traffic jam, with an inter-vehicle distance of 5 m, there can be more than 1000 vehicles within the same region.

In this article, our focus is on VANET applications and related technical issues. In essence, vehicles in a VANET must receive and send data quickly. We discuss how this can be accomplished in VANETs in the physical/medium access control (PHY/MAC) section. VANETs also must be able to communicate with all parties concerned. Approaches to meet-

[1] *Minimum security distance between two vehicles cruising at 130 km/h.*

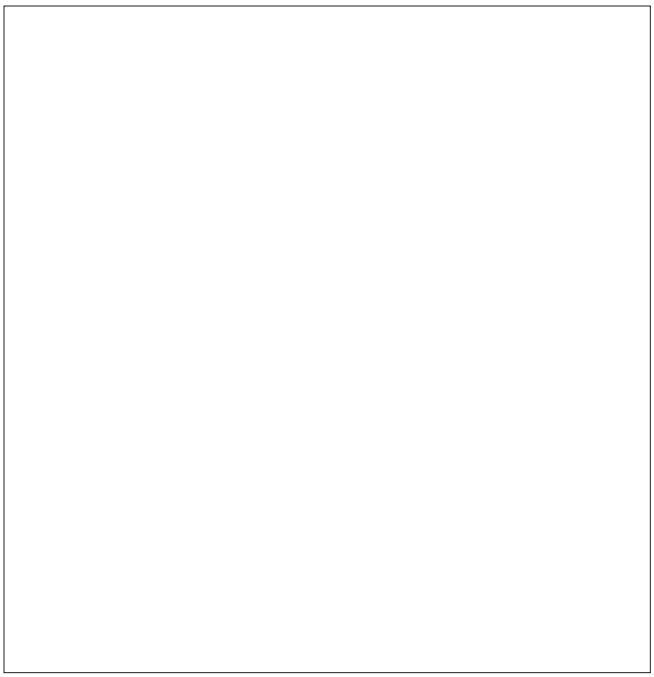


Figure 1. *Two basic kinds of VANETs, infrastructure-based and ad hoc.*

ing this requirement are presented in the routing and data dissemination section. Then, we discuss the suitability of TCP/IP[2] for VANETs. Vehicles in a VANET also require secure communications, and this aspect is discussed in the security section. Dimensioning and performance analysis must be performed on VANETs, and applications also must be tested. We address this aspect in the simulation section. Before concluding, we give a short review of a few research projects and organizations dealing with VANETs.

Applications

VANET applications can be divided into two major categories. Applications that increase vehicle safety on the roads are called safety applications. Applications that provide value-added services, for example, entertainment, are called user applications. In this article we concentrate only on applications with an important wireless networking component.

Safety Applications

Safety applications can decrease significantly the number of road accidents. According to some studies [6], 60 percent of accidents could be avoided if a driver were provided with a warning half a second before the moment of collision. There are three major scenarios in which safety applications could be very useful.

- Accidents: Vehicles travel at a high speed on major roads. This gives drivers very little time to react to the vehicle in front of them. If an accident occurs, the approaching vehicles often crash before they can come to a stop. Safety applications could be used to warn cars of an accident that occurred further along the road, thus preventing a pile-up from occurring (see, e.g., [7]). A safety application also could be used to provide drivers with early warnings and prevent an accident from happening in the first place.
- Intersections: Driving near and through intersections is one of the most complex challenges that drivers face because two or more traffic flows intersect, and the possibility of collision is high. In 2003, according to the U.S. Department of Transportation (DoT), intersection crashes accounted for more than 45 percent of all reported crashes and 21 percent of fatalities, that is, 9213 fatalities occurred at intersections in the United States [8]. The number of accidents would decrease if a safety application warned the driver of an impending collision. The driver then could take action to prevent it (see also the European project PReVENT/Intersafe [4]).
- Road Congestion: Safety applications also could be used to provide drivers with the best routes to their destinations [9]. This would decrease congestion on the road and maintain a smooth flow of traffic, thus increasing the capacity of the roads and preventing traffic jams. It also could have the indirect effect of reducing traffic accidents [10] because drivers would be less frustrated and more inclined to follow traffic regulations.

User Applications

User applications can provide road users with information, advertisements, and entertainment during their journey. Two basic user-related applications are described below.

- Internet Connectivity: Constant Internet access has become a daily requirement for many of us and because many user applications also require Internet connectivity, providing this facility to vehicle occupants and other VANET applications is important. Moreover, this means that the usual business framework will be present seamlessly in vehicles, without a requirement for specific redevelopment.
- Peer-to-Peer Applications: To alleviate boredom, peer-to-peer applications also are an interesting idea for VANETs. Passengers in the vehicles could share music, movies, and so on and chat with each other and play games. They also could stream music or movies from special servers during long journeys.

As a final point, applications developed for VANETs must ensure that problems inherent in VANETs are invisible to the users. In the following sections, we look at some solutions that were suggested.

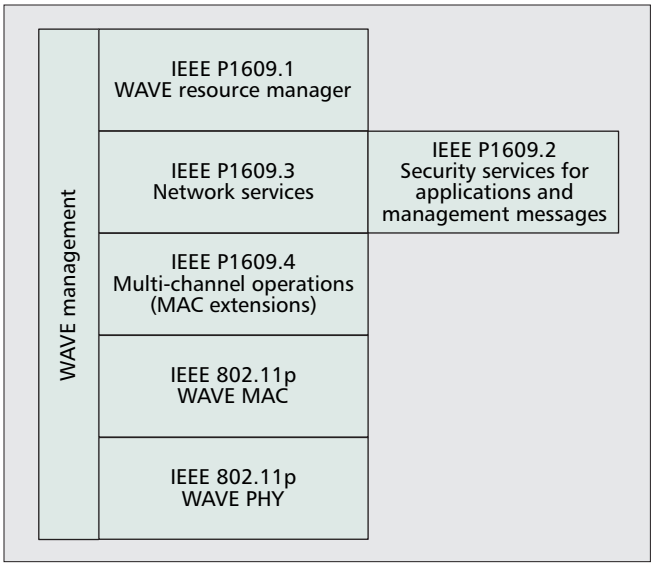
PHY/MAC Layer

Both radio (very high frequency [VHF], micro, and millimeter waves) and infrared waves have been used in experimental V2V systems. Infrared and millimeter waves allow communication only in line of sight;[3] VHF and microwaves allow broadcast communications. VHF can provide long links but at low speed; the mainstream is microwaves. In the United States, 75 MHz in the 5.9 GHz band is allocated for VANETs; in Europe and Japan, the spectrum allocated to VANETs is in the 5.8 GHz band. In Europe, 10 MHz also is available between 2010 and 2020 MHz for vehicle communications.

In the PHY/MAC layer for a VANET, three difficult problems must be solved. The first is how to offer robust transmission between vehicles and an efficient sharing of the radio medium. This is a special case of the same problem in MANETs but with the peculiarity that VANETs are usually linear networks. The second problem comes from the fact that

[2] *Transport and routing layer of the Internet protocols.*

[3] *Usually, directional.*



■ **Figure 2.** *IEEE 802.11p in the IEEE P1609 standard family.*

there may be a large variation in the density of nodes in a VANET. For instance, in traffic jams or just after an accident, the density of nodes may increase considerably. The third problem concerns the support of emergency applications; in fact ensuring quality of service (QoS) is difficult in a wireless environment. We now present existing research studies in these three fields.

Physical Layer

Most current experiments in V2V and V2I use the IEEE 802.11a, b, or g technology. The forthcoming IEEE 802.11p standard uses a physical layer based on orthogonal frequency-division multiplexing (OFDM). This physical layer will be very similar to the physical layer of IEEE 802.11a. The major difference will be that the physical parameter values are doubled in the time domain to decrease the inter-symbol interference caused by the multipath delay spread and the Doppler spread effect. IEEE 802.11p targets a transmission range between 300 m and 1 km. The signal bandwidth thus is reduced from 20 to 10 MHz, and the data throughput ranges from 3 to 27 Mb/s instead of 6 to 54 Mb/s. There are only a few proposals [11, 12] that describe solutions not based on the IEEE 802.11 technology. Among these, the European project FleetNet [11] proposes to use another physical layer based on universal mobile telecommunications system (UMTS) terrestrial radio access time division duplexing (UTRA-TDD) radio hardware [13]. This approach is shown in [14] to offer better performances in terms of bit error rate than a solution based on IEEE 802.11b, both in situations of high relative velocity and large variations in multipath delays.

Medium Sharing

In VANETs, the main requirement for the PHY/MAC layer is to offer robust transmission between vehicles on a perturbational [15–17] and shared medium. There are two main solutions to sharing a medium. The first is to use controlled-access protocols. In such protocols, access to the medium is decided in advance; one example of such a protocol is the Time Division Multiplexing Access (TDMA) protocol, in which every network node has a dedicated and predetermined time slot to send its packets. The second way is to use random access protocols. With these protocols, a node tries to send its packet and if a collision occurs, that is, the transmission interferes with another simultaneous transmission, the packet cannot be received correctly by the recipient. The node must send the packet again. The forerunner of random access protocols is Aloha [18]. In this protocol, a node sends a packet whenever it has a pending packet. If the packet collides, the node retransmits the packet after a random delay. A more advanced protocol is the Carrier Sense Multiple Access (CSMA) protocol [19]; in this protocol, a node verifies that there is no ongoing transmission before sending its own packet. A good overview of multiple access schemes can be found in [20].

It is not difficult to observe that due to the dynamic and open nature of VANETs [20], random access protocols are preferable to controlled access protocols. In accordance with this observation, the IEEE 802.11 access method distributed coordination function (DCF) is used widely as a basis for V2V communications. IEEE 802.11 uses a CSMA protocol with a per packet MAC acknowledgment. This acknowledgment, at a low level, improves the robustness of the transmission but also can detect collisions indirectly.[4] The access scheme of IEEE 802.11 also includes an optional handshake scheme performed between the source and the destination to improve the performance. This scheme is particularly useful when there are hidden nodes. Node *B* is said to be hidden from node *A* when *B* is not within carrier-sense reach from node *A*. In a CSMA protocol, *B* can transmit while A is already transmitting, and thus, node *B* can corrupt the transmission of node *A* to node C located between *A* and *B*.[5] To cope with this problem, the request-to-send/clear-to-send (RTS/CTS) handshake mechanism [21] often is used. Before the transmission of a packet, sender A sends an RTS packet to recipient *B*. If *B* is ready, it responds with a CTS packet. This warns the nodes in the vicinity of *B* of the transmission and thus stops hidden nodes from transmitting their packets.

Using the IEEE 802.11 access method and operating in the 5.9-GHz band,[6] the dedicated short range communications system (DSRC) [22] was proposed recently. DSRC is a short-to-medium range communications system that supports both safety and user applications in roadside-to-vehicle and vehicle-to-vehicle communication environments. DSRC is now standardized as 802.11p within the IEEE 802.11 working group, and it also is the MAC and PHY layer of the IEEE P1609 standard family — the IEEE standard for wireless access in a vehicular environment (WAVE). The whole structure of the IEEE P1609, and the place of IEEE 802.11p inside it, is shown in Fig. 2. In this figure, we can see that 802.11p operates below several management protocols in charge of resource management, networks services, channel selection, and security.

To the best of our knowledge, most current trials of V2V networks use the IEEE 802.11 technology [17, 23] and its CSMA sharing technique. There are also a few proposals to

[4] *If a packet is not received due to a collision, no acknowledgment packet can be sent.*

[5] *Depending on node C's position and on the capture conditions for the reception at node C.*

[6] *5.8-GHz band in Japan and Europe.*

[7] *In a slotted protocol, access is granted on predefined time intervals called slots; in slotted Aloha, the available throughput is actually doubled compared with the throughput obtained with the usual Aloha; see [20].*

[8] *i.e., collisions with hidden nodes.*

use techniques derived from third generation (3G) telecommunication systems. For instance, the European project, FleetNet, proposes an approach based on slotted Aloha. Slotted Aloha performs better than standard Aloha and also is more compatible with a 3G-like system that generally uses a TDMA with time slots.[7] The FleetNet project uses reliable reservation-Aloha (RR-Aloha) [24] as the access scheme. RR-Aloha is a variation of the well known R-Aloha protocol [25]. R-Aloha itself is an improvement of the slotted Aloha protocol where nodes perform a reservation to acquire slots. RR-Aloha adds an additional mechanism to R-Aloha to inform nodes of the status of the slot (free or used) at two hops. A slot at a given location can be used only when it is not used by any nodes two hops away from the given location. This ensures that the transmission in one slot will not collide with another transmission in a more distant slot. This technique should avoid hidden collisions.[8] The approach seems promising, although it is very difficult to evaluate its performance with highly mobile nodes because it is difficult to be sure of the accuracy of the two-hop neighborhood of a node.

We also found an academic study [26] that proposes a token protocol similar to 802.4 to solve the issue of radio resources. The operation of such a protocol is not realistic in VANETs because the nodes are highly mobile and transmission conditions are difficult. The performance evaluation provided in [26] does not even consider mobility, and [26] is very far from proving that the proposed access scheme is convenient for VANETs.

In this section we present the two main medium-sharing approaches that could be used for V2V communications: the random one (e.g., CSMA-like) and the controlled one (e.g., TDMA-like). However, due to the dynamic and open nature of VANETs, a random approach is better suited to V2V communications. CSMA was adopted by IEEE 802.11, as well as by IEEE 802.11p as the medium access method. IEEE 802.11p most probably will be the default technology for VANETs because it has received backing from industry. RR-Aloha and similar schemes probably could be successfully used in VANETs also. However, the issue of access schemes in an ad hoc network is not very well understood, even though a few theoretical studies, such as [27, 28], have provided very interesting results. In fact the main problem stems from the fact that in ad hoc networks, access schemes must handle both time and space sharing.

Coping with High Node Density

Another major problem in V2V and V2I communication is the high density that a network can reach, for example, during a traffic jam or after an accident. A similar problem already was studied in access protocols for wired networks. Various schemes were proposed to increase the maximum throughput of these protocols (see [20]). However, the problem in a V2V network is more complex because V2V networks also allow spatial reuse and thus offer another variable that can be adjusted. Many studies attempted to tackle this issue of high density [29, 30]. In [29], the idea is to divide the road into very small segments to which a time slot can be allocated. For a vehicle in a given segment to use more than the bandwidth provided by the time slot of its segment, the protocol described in [29] allows a vehicle to use the time slots of the segments up to the preceding vehicle. In [30], the main idea is to adapt the carrier sensing together with the transmission area; [30] still uses a slotted approach. If a vehicle cannot find an available slot in a given sensing area, it decreases its sensing area until there is an available slot in the current area again. The transmission area is reduced together with the sensing area to avoid a hidden collision. A similar technique for CSMA protocols could be designed.

Certain studies tried to use directional antennas for V2V communication. The expected gain in throughput was shown to be between

$$\sqrt{\frac{2\pi}{\alpha}} \text{ and } \frac{2\pi}{\alpha}$$

in a two-dimensional MANET when the nodes transmit in a sector of angle α; see [31]. The gain in throughput was shown to be between

$$\sqrt{\frac{4\pi^2}{\alpha\beta}} \text{ and } \frac{4\pi^2}{\alpha\beta}$$

in a two-dimensional MANET, if one uses a directional antenna transmitting in a sector of angle a and a reception antenna receiving in a sector of angle β; see [31]. In [32], the performance of a MAC protocol (directional MAC, [DMAC]) using a directional antenna for transmission is studied in the context of V2V communications. The gain is shown to be significantly lower than the theoretical gain foreseen in [31] and even the simulated gain of the DMAC protocol [32]. The reason for this discrepancy between prediction and real performance is due to the fact that V2V networks are mainly linear networks, whereas the theoretical gain of directional antennas and the performance of DMAC are measured in two-dimensional MANETs. The interest of directional antennas appears to be rather small in VANETs.

QoS and Time Critical Traffic

Another important requirement for VANETs is for vehicles to exchange important messages immediately and efficiently (mainly for safety reasons). The probability of collision and the corruption of emergency messages must be low. The problem is that current wireless local area networks (WLANs) mostly handle data without time constraints. They have no real QoS or real-time traffic support. In VANETs, there could be many vehicles traveling along the road and if an emergency occurs, for example, a crash; the group of vehicles affected by the event could change and increase very quickly. If every vehicle starts broadcasting emergency messages, it could cause a broadcast storm, leading to congestion on the channel. This would make detection and differentiation of emergency messages difficult.

Several studies of the MAC layer for V2V focus on the mechanisms to send time-critical traffic for emergency applications, for example, during a car crash. Two classes of solutions were proposed to solve these issues. One possibility is to change intelligently the number of vehicles transmitting the emergency messages and the rate at which they are transmitting the messages. The second solution is to change the transmission range of the emergency messages as the number of affected vehicles increases. Liu *et al.* [33] proposed a communication protocol that falls into the first class. They utilize repeated broadcasts for reliable delivery of emergency messages. The transmission rate depends upon the transmission range, maximum speed, and the deceleration capability of the cars and the channel conditions. The messages include the geographical position, speed, acceleration, and direction. The initial rate of transmission is high but then decreases to cater to other cars. They also eliminate redundant emergency messages utilizing the natural chain of events. The simulation

results show that the delivery delay is not significantly affected by the increase in cars, and the number of emergency messages also remains reasonably stable. The proposal of Torrent-Morena *et al.* [34] falls into the second category of solutions. They suggest that the vehicles transmitting emergency messages in a given area decrease their power by the same ratio so that there is no congestion, and safety messages have a higher probability of being delivered.

Lessons Learned

There have been many studies in the area of the PHY/MAC layer for VANETs, and significant results were obtained. Random access techniques and the IEEE 802.11 technology dominate in the trials and in standardization activity; IEEE 802.11p is expected to be the dominant standard for VANET communications. However, there is still a lack of a profound understanding of protocols where both time and space must be shared in MANETs and consequently, in VANETs. Nor is there an established model (an analytical or at least, a simulation model) that can be used to compare solutions on an objective basis or a set of precise requirements for the PHY/MAC of VANETs.

Routing

Intense research was performed about routing in MANETs over the last decade. A good survey can be found in [35], and the reader with limited knowledge in this area would be well advised to read it. The issues or properties in the routing area that are specific to VANETs are listed in the following.

- Generally, VANETs are linear networks, and the nodes are highly mobile with possibly predictable movements. Moreover, the assumption that the location of the nodes is known is realistic in a VANET.[9] This offers the possibility of adapting or optimizing existing routing protocols or even designing new protocols.
- Due to the high mobility of the nodes, connectivity is a real challenge. Routing protocols for VANETs must cope with the partitioning and merging of networks. Also, during the initial deployment of a VANET, there is sparse network connectivity, and this must be handled properly.
- In VANETs, vehicle mobility can be used to improve the performance of the network; in fact, mobility increases the throughput in MANETs, as is shown in [36].
- For safety applications, VANETs require broadcast protocols to flood information efficiently and reliably within a given area.

To review these points, first we investigate routing for user applications in VANETs. Then we deal with Internet connectivity for VANETs. We end this section with a discussion of routing for safety applications, in which we discuss efficient and reliable flooding in VANETs.

Routing for User Applications

User application requirements have not been clearly defined yet. Applications can use either unicast routing or multicast routing. Our interest in this section is to see how a route can be provided between a source and a destination vehicle in such a way as to ensure communication. We review the classical MANET unicast routing protocols. Then, we present geographic routing, which takes into account the current geographical positions of the source and the destination cars to route the data. We also present how data routing can be enhanced by predicting radio link changes and thus prevent link breakages during communications. Finally, we introduce message-ferrying techniques to improve data forwarding between disconnected vehicle networks.

Due to intensive research in the field, a number of unicast routing protocols were developed especially for MANETs; for example, optimized link state routing (OLSR) [37], ad hoc on-demand distance vector (AODV) [38], dynamic source routing (DSR) [39], and so on. These protocols can be divided into two basic types: reactive and proactive. Reactive protocols discover the route when there is a data packet to be sent. Generally, a control packet is flooded from the source, and the path of this packet toward the destination node creates the route to the destination. Hence, there is a delay before data can be transmitted. Proactive protocols, on the other hand, maintain a correct routing table at all times by sending periodic control messages that contain topology information. Thus, with a proactive protocol, routes are available without delay. Both reactive and proactive protocols primarily try to find short routes,[10] and they usually use the shortest path algorithm. A somewhat exhaustive description of routing algorithms for MANETs can be found in [40, 41]. To the best of our knowledge, there has been no systematic comparison of reactive and proactive protocols for VANETs. However, [42] compares the overhead incurred by reactive and proactive protocols given the following parameters: the network graph, the number of active connections, and the mobility of nodes. The length of routes (source-destination) also is compared, and even though it [42] is not devoted specifically to VANETs, this information could be useful for comparing protocols in VANETs.

As already stated in the introduction, VANETs can encompass a large number of nodes. To cope with this issue, geographic routing [43] was proposed to reduce the routing state of each node.[11] In fact, in geographic routing, the protocol makes forwarding decisions based on the geographical position of the destination of a packet. A relaying node must know only its own position, the position of the destination, and the positions of its one-hop neighbors. Geographic routing protocols are not required to maintain explicit routes and thus scale well, even with dynamic networks. Therefore, geographic routing is potentially very interesting in a VANET because vehicles can be assumed to know their positions through a global positioning system (GPS). It must be noted that geographic routing requires a location service capable of providing a node with the position of its one-hop neighbors and the destination of the packet to be relayed. Such a service can be obtained if each node regularly floods, as proposed in [44]. In addition to offering a scalable routing approach, geographic routing also can optimize the routing path from the origin node to the destination node. For instance, the next relay can be selected to maximize the progress of the packet toward its destination (see e.g., [28, 45–47]). In [48], one can find a survey on geographic routing techniques but to our knowledge, there is no published study comparing geographic routing protocols with usual routing protocols for VANETs. However, this technique appears to be attractive; the Car2Car Consortium (C2C-CC) uses it [49]. Unfortunately, the C2C-CC has not disclosed detailed specifications of the geographic

[9] *Most new cars can be expected to have a global positioning system (GPS).*

[10] *Usually, the protocols search for routes with the smallest number of hops, but additional or other criteria also can be used.*

[11] *Number of routing entries.*

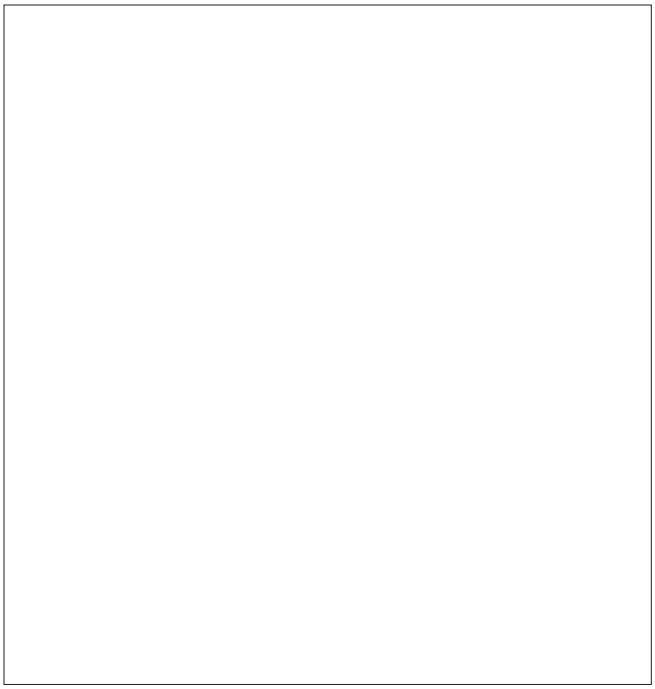


Figure 3. *Drivethru Internet. When a vehicle is in range it is able to communicate with the Internet. The drive-thru proxy allows the client application to work without modification; connections are maintained while a vehicle transits from one connectivity cloud to the next connectivity cloud.*

routing protocol it intends to use. The study proposed in [50] introduces the concept of conditional transmission: instead of transmitting addresses, a message is sent with conditions used to determine whether it must be retransmitted. This technique can be seen as a generalization of the geographic routing technique.

Due to the high mobility of nodes in VANETs, network partitions can occur frequently, and this results in route unavailability, which in turn causes high data packet loss. The effects of such partitions are minimized by predicting vehicle mobility and message queuing until a route is available. Wu and Harms [51] propose a proactive flow-handoff method. They try to minimize the effects of partitions. The main idea is that during data transmission, each node along the path that is used monitors the connectivity to its previous and next nodes and predicts the link lifetime to its next node. If it predicts that this link lifetime is too short, it will search locally for another path with a longer link lifetime and hand over the flow to the newly found path. If that is not possible, a message is sent back to the source, and it can initiate a new route discovery phase. However, every node must know its own location, its own velocity, and the global time. It also should know the approximate positions and velocities of the other nodes. Moreover, prediction becomes difficult in complex environments such as cities. In [52], a movement prediction technique (movement prediction routing) is used to improve the connectivity obtained with the OLSR routing protocol. The idea is to select the links according to an estimated value of their lifetime. This estimation easily can be obtained if the positions and velocities of the nodes are known. Results given in [52] show that a great improvement in performance can be achieved when the movement prediction technique is used.

In addition to the obvious problems caused by the high mobility of nodes, there will be another foreseeable connectivity problem in V2V networks when the VANET technology initially is deployed. Roads will contain few equipped vehicles, and this will result in sparse and partitioned networks. To solve this problem, researchers have proposed using the mobility of the vehicles to counterbalance the sparsity of the network [53, 54]. Wu *et al.* [53] propose a mobility-centric approach for data dissemination (MDDV) in VANETs that exploits the mobility of each vehicle to improve network connectivity. It requires that vehicles have access to information about their own location through a map database and GPS information. One or more vehicles moving in the direction of the destination store the message. This vehicle is called the message head. Only the message head can forward the message. Each message has information about its approximate current location and generation time. A vehicle makes the decision about storing, discarding, or forwarding a message based on this information. On the other hand, dedicated vehicles can be used to prevent network partitioning. Several message-ferrying techniques were proposed for sparse MANETs. Tariq *et al.* [55] propose an interesting scheme, where a special node called the ferry, facilitates the connectivity in a MANET by ferrying the messages for other nodes. They have carried out many simulations to show that this scheme is fair and provides good performance. Such a system might be interesting in sparse VANETs where network partitioning is a particular problem. For example, the concept could be implemented by using traffic police vehicles to act as message ferries.

Internet Connectivity

Whereas the previous issue was to maintain connectivity between the nodes of a VANET, the issue here is to maintain Internet connectivity for vehicles within a VANET.

Ott and Kutscher [56] provide WLAN-based Internet access for vehicles based on the drive-thru architecture. They identify three phases when a vehicle is passing through a connectivity cloud. The entry and exit phases provide low data rates, but the middle phase provides up to 5 Mb/s. Hence, a dedicated drive-thru proxy on the Internet, together with a support subsystem on the vehicle, enables client-server applications, for example, e-mail and Web browsing, to work without modification. The drive-thru architecture is illustrated in Fig. 3.

Namboodiri, *et al.* [57] suggest using multi-homed vehicles to act as gateways together with predictive protocols. The mobile gateways would share their bandwidth and computing power to provide other vehicles with connectivity to the Internet and other resources. Predictive routing would increase the duration of the link to the gateways. According to the authors, such protocols would start looking for a new route before the current route breaks, thus reducing the number of link breakages.

Solutions requiring infrastructure gateways would require a heavy initial investment but would be easier to manage. Additionally, the development of special protocols and applications also would benefit from the knowledge that these gateways would be present after a specific distance. The second approach [57] has the drawback that the users would need an incentive to act as gateways for others because they would be sharing their bandwidth and computing resources. A solution that could switch between the two approaches would be the most versatile and deployable.

The NEtwork MObility (NEMO) approach developed by the Internet Engineering Task Force (IETF) is interesting for VANETs moving from one access network to another while trying to keep connected. However, within VANETs, connectivity is very dynamic, leading to network merging or partitioning; and thus the approach adopted in NEMO [58, 59] is probably not suitable. Moreover, this approach was not opti-

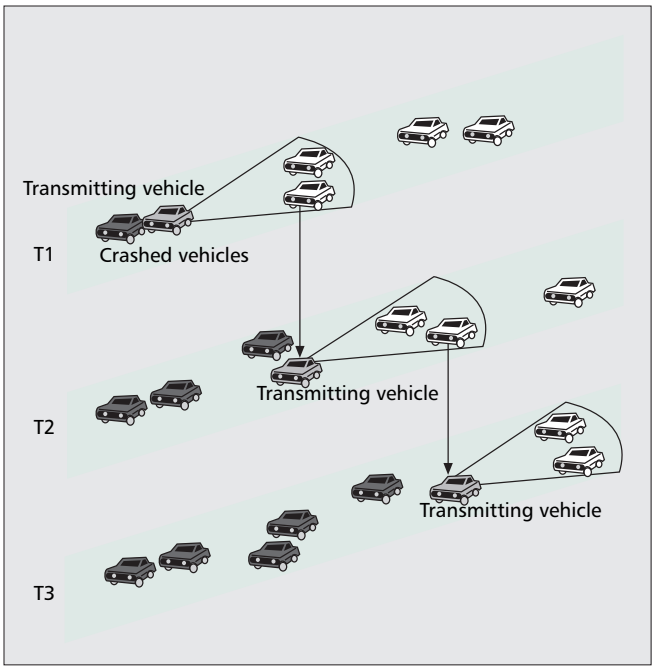


Figure 4. *Progression of the information with the Biswas scheme. The black cars are aware of the accident, the grey car is relaying the information and the white cars do not know about the accident yet. Notice that the relaying car is not always the furthest from the previous relay; at T1, car 1 acts as the relay even though car 2 is further from the current relayer.*

mized in terms of routing. MANEMO [60, 59] combines a MANET approach and a NEMO approach and probably would be more suitable, but the development of this technology is just beginning.

Routing for Safety Applications

As seen previously, safety applications require broadcast routing schemes. There are several multicast protocols that were proposed for MANETs or directly derived from MANET unicast protocols, for example, Core Assisted Mesh Protocol (CAMP) [61], On-Demand Multicast Routing Protocol (ODMRP) [62], Multicast AODV (MAODV) [63], and Multicast OLSR (MOLSR) [64]. None of them, however, was carefully evaluated for VANETs. Moreover, these protocols are multicast protocols and not the efficient broadcast routing protocols required by VANET safety applications. In addition, emergency messages must be transmitted with stringent time constraints that require a rapid reaction time from the routing protocol. Therefore, the delay implicit in reactive protocols is unacceptable. A proactive protocol would seem a more suitable way to relay safety application messages. We must bear in mind, though, that proactive protocols consume a significant part of the available bandwidth simply to maintain connectivity. Special consideration should be given to OLSR because this protocol was designed specially to optimize the flooding of control messages. The scheme is based on multipoint relays and could be used to broadcast emergency messages in VANETs.

Biswas *et al.* [65] produced the first in-depth study into how to efficiently handle safety packets. This article proposes a broadcast technique based on geographic routing (using additional directional information). When a vehicle receives the safety packets, it starts a periodic broadcast of these safety packets. In this way, the vehicle propagates the safety information. But if this vehicle receives the same safety packets from a vehicle behind it, it stops transmitting so as to avoid transmitting unnecessary packets. In fact, in this case there is at least one vehicle behind it to propagate the safety packets, as shown in Fig. 4. It should be noted that it is not necessarily the vehicle that is the farthest from the previous relay that acts as a new relayer. In [65], safety packets are given higher priority than the background data traffic generated by user applications. The simulation results show the importance of this traffic prioritization to provide good performance for the safety application.

The study in [66] compares three techniques to disseminate emergency data within a platoon of cars. The first technique is pure flooding, the second is the multipoint relay (MPR) diffusion technique of OLSR [37], and the third is a geographic-aware flooding mechanism derived from the work of Biswas *et al.* [65]. The simulation in [66] shows that flooding significantly outperforms the two other schemes for delivery delay and the percentage of successfully transmitted packets. However, the bandwidth used by flooding is far greater than that used by the two other schemes. The MPR technique consumes the least bandwidth by far, but the delivery delays obtained are too great for safety applications. A simple modification of the MPR technique allows good delivery delays to be obtained while still consuming far less bandwidth than pure flooding.

Lessons Learned

There are a significant number of contributions in the area of routing for VANETs, and some interesting results already were obtained. One of the important results concerns the possible utilization of the mobility of the vehicles to improve network connectivity. Another important aspect of the contributions in this area is the study of geographic routing protocols, although we have not found any published papers with convincing arguments that conclude that geographic routing is the most efficient technique in VANETs. The fact that the C2C-CC has adopted a geographic routing protocol is probably a hint in favor of geographic routing. But there is a lack of fully specified geographic routing protocols for VANETs. Such a protocol could be used to objectively draw a comparison with existing protocols. The choice of routes, bearing in mind mobility, was well studied in reactive and proactive protocols. Nothing, however, was proposed for geographic routing protocols. Such a study is sorely needed. Moreover, there have been no investigations concerning realistic propagation in VANETs using models that take into account phenomena such as deep fading and so on. These may cause a lack of connectivity for up to ten seconds or more. Such investigations could lead to the development of special routing techniques or mechanisms that can be added to existing routing schemes to avoid long periods without connectivity. The linear shape of most VANETs and the potential consequences on the design of routing protocols is something that has not been deeply analyzed yet.

Data Dissemination

Data dissemination is the transportation of data to the intended recipients while satisfying certain requirements such as delay, reliability, and so on. These requirements vary, depending upon the data being disseminated. Because they are different for safety applications and for user applications, we discuss them separately. Data dissemination in VANETs is a complex subject that is linked to the MAC and routing issues and brings additional possibilities such as the use of the infrastructure support and the possibility of aggregating data. The

main issue for data dissemination is that a simple query or on-demand methodology for disseminating data does not suit VANETs due to their high mobility and network partitions. Moreover, data dissemination in VANETs usually cannot use group addresses but must rely on the locations of nodes to determine the nodes in the delivery group.

Data Dissemination in Safety Applications

Safety applications require that certain data be disseminated in a geographical area under all conditions. The reason for this is that the relevance of information in safety applications in a location decreases with the distance to that location. Therefore, there have been several proposals to limit data dissemination, for example, using hop count and so on, which make up the first class of proposals. Proposals belonging to the second class use vehicle location information to help in data dissemination.

Bronsted and Kristensen [67] propose two zone dissemination protocols that aggregate the data and distribute it only within a bounded geographical area. Hence, it is a form of flooding-based geocasting. It uses hop counts to limit the transmissions and a sequence number to stop retransmission of the same packet by a vehicle. A flooding zone also is embedded in every packet specifying a geographical area. Fracchia *et al.* [68] propose the HELLO-estimated location-based procedure (HELP). The basic idea of HELP is that each node estimates the position of its neighbors by exploiting the information exchanged by routing algorithms through the use of the HELLO packets.[12] Then, the positions of the neighbors are used to decide whether a message should be forwarded or not. It is assumed that the routing layer maintains neighborhood state information, recording for each neighbor, a tuple (the node identifier, the time of the HELLO transmission, and the position and the speed of the node at the time of the HELLO transmission).

The first class of solution is simpler and faster, but in the second approach, although the use of GPS and map information makes the dissemination more accurate, it also makes it complex. There have been no studies that compare the performance of the two approaches in a precise manner. Zone dissemination protocols are of particular interest and should be the subject of further investigation.

Data Dissemination in User Applications

Schemes for data dissemination in user applications should hide the high mobility of VANETs and network partitions from the applications. The problem is that the highly mobile nature of VANETs makes locating the required data difficult. After the data is found, frequent network partitioning can render the data unavailable for an unknown period of time. Also, due to the wireless medium, bandwidth can be very limited, and download times unreasonably long. Two classes of solutions were proposed. The first class uses the infrastructure support and available technologies to disseminate data. The second class tries to build a completely independent system.

The first approach is used by Ghandeharizade *et al.* [69] who try to solve the problem by using multi-homed vehicles and cooperative users. A multi-homed vehicle is one that has more than one way of accessing the wireless medium, for example, a cellular connection, as well as an IEEE 802.11 wireless connection. They proposed a policy framework for content availability in vehicular ad-hoc networks (PAVAN) that uses the cellular system to collect content and mobility information from vehicles. This data is then aggregated and disseminated to the vehicles. Then, the users in the vehicles can make their choice and use the ad hoc network for the actual exchange of files if it has better bandwidth. To ensure a better choice for the user and provide high availability, data can be replicated in different cells.

The second approach is used by Repantis and Kalogeraki [70] who propose a data dissemination scheme for large-scale, mobile, and unstructured peer-to-peer networks that is suitable for VANETs. They propose an adaptive, content-driven routing and data dissemination algorithm for intelligently routing search queries in a peer-to-peer network. A node builds and maintains a content summary of its local data and adaptively disseminates it to the selected peers. Then, a peer that does not have the required data locally can use these summaries to determine if one of its peers can provide the requested data or service. If no such peer is found, then the query is forwarded to a random selection of peers. They also evaluated different dissemination strategies for content summaries. Their conclusion is that local summaries and summaries received from remote peers should be disseminated to adaptively selected peers to obtain the best results.

The first approach requires the infrastructure to be present. Hence, these solutions work only while the vehicles remain in the area covered. This might limit the usefulness of the scheme. In contrast, the second approach does not have this restriction. However, its applicability in sparse VANETs must be studied further. A solution that can amalgamate both these ideas would be interesting for VANETs. Another problem that requires attention is the accurate prediction of content in highly mobile VANETs.

To obtain a proper comparison of dissemination protocols, metrics must be developed that reflect their important properties. S. Kapadia [67] introduced two interesting metrics. First, when a node first learns something about a phenomenon further along the road, the information distance is the distance from the position of this node to the phenomenon in question. The information distance is a measure of the distance of the warning the driver of the vehicle can expect. Second, the awareness percentage for a particular location is the fraction of nodes passing the location that had information about the location before entering it. These metrics are particularly useful for safety applications. Other metrics for data applications should be defined.

Lessons Learned

Data dissemination in a VANET is a difficult subject linked to the MAC and routing issues but with additional complexity brought about by the possibilities of the infrastructure support and the possibility of aggregating data. In the future, almost all cars likely will have a type of navigation system using a GPS. Hence, researchers should concentrate on dissemination schemes for safety applications that use location information effectively. However, during the initial deployment of a safety application in a VANET, the penetration ratio will be small. Thus, during this interim period, the data dissemination scheme also should be able to function adequately without this information. For data dissemination in user applications, an architec-

[12] *The HELLO packets are used by the routing protocols to build the neighborhood of the nodes.*

[13] *IPv6 Internet Protocol version 6.*

[14] *This is mainly a consequence of hidden collision and the back-off strategy used by wireless access protocols.*

ture similar to a PAVAN [69] is an attractive solution. Because it uses the available infrastructure efficiently and also uses V2V communication, it can be deployed widely. A purely P2P scheme does not use the infrastructure available in the VANET and so would not enable users to have a wide variety of choices because their choices would be limited to their vicinity.

TCP/IP Stack

Because the Transport Control Protocol/ Internet Protocol (TCP/IP) stack is not well suited to wireless networks, this is equally the case for VANETs. IP encapsulation introduces a large overhead, especially when IPv6 is used.[13] Nor is the use of short packets recommended in wireless networks because there are long synchronization times. Moreover, many research studies have shown TCP to be quite unsuitable for MANETs, and hence for VANETs, because it was designed for wired networks. The reasons for this inadequacy are mainly the following:

- The access protocols for wireless networks often lack fairness [71, 72, 73],[14] which also can cause unfairness at the transport layer [74].
- In wireless networks, it is very difficult to discriminate between congestion and packet loss due to transmission errors.
- In dynamic networks such as VANETS, losses of connectivity are interpreted as network congestion, and this can greatly decrease the throughput of the network when TCP is used.

Several modifications to TCP were proposed to adapt it to wireless ad hoc networks (e.g., VANETs). An initial approach is to extend TCP. Most of the proposed TCP extensions are end-to-end approaches with some sort of feedback mechanism. Examples of this approach include: TCP-failure (TCP-F) [75], TCP-explicit link failure notification (TCP-ELFN) [76], TCP-BuS [77], ad hoc TCP (ATCP), and split-TCP [78].

TCP-F [75] uses a feedback mechanism in the form of route failure notifications. This notification is sent by the node when the route breaks and causes the TCP-F sender to enter a "snooze" state. In this state, the timers and windows are frozen, and no packets are sent. A route failure timer is started with the worst-case route reconfiguration time. This depends on the routing protocol, network size, and network dynamics. When this timer expires, the TCP-F sender goes back into the connected state, starts the timers, and sends the buffered and unacknowledged packets. However, if the TCP-F receiver rejoins the network or an intermediate node finds an alternative route before the expiry of the timer, it sends a route reestablishment notification. This notification causes the TCP-F sender to assume that the network returned to its original state, and so it sends the packets into the buffer and avoids a slow start. It uses normal congestion control mechanisms when not in the snooze state. TCP-F has two major disadvantages. It adds another state to TCP and hence requires modifications to all nodes. The second disadvantage is that after a new route has been acquired, the congestion window may not represent the transmission rate acceptable to the network and the TCP-F receiver.

TCP-ELFN, TCP-BuS, and ATCP use similar concepts, whereas split-TCP splits long TCP connections into shorter segments with special intermediate nodes — proxies — as the terminating nodes. Other solutions also were proposed that build up a completely new transport layer protocol from scratch. Two examples of this approach are Application-Controlled Transport Protocol (ACTP) and Ad Hoc Transport Protocol (ATP).

ACTP is similar to User Datagram Protocol (UDP) with feedback on the delivery of packets and state. In ACTP, reliability is handled by the application layer; the feedback on delivery status is provided by ACTP. It does support priority but does not implement it, and the lower layers must provide that service. The advantages of ACTP are that the application can choose the required level of reliability, and it is lightweight and scalable. In addition, throughput is not overly affected by path breaks because there is no congestion window. However, its major disadvantage is that it is not compatible with TCP. ACTP also can cause heavy congestion in very large networks because there is no sophisticated congestion control mechanism.

ATP differs from TCP mainly in its use of cross-layer coordination to improve performance. It performs rate-based transmissions. It also decouples congestion control and reliability, as well as performing assisted congestion control. It does this by obtaining the congestion information from the intermediate nodes. The intermediate nodes attach this information to the packet, and then the information is collated and sent back by the ATP receiver in the acknowledgment. It also sends back flow control and reliability information. The advantage of ATP is that it has improved performance compared to TCP, and it also avoids fluctuation of the congestion window. One of its major disadvantages is its lack of interoperability with TCP.

Lessons Learned

Despite efforts to improve the performance of the TCP/IP stack for MANETs through the use of various additional schemes, the inadequacy of the TCP/IP stack for MANETs remains apparent. This led the U.S. Department of Defense to initiate a new research program called Control Based Mobile Ad-Hoc Networking (CB MANET) [79]. This research aims to design a completely new IP stack for MANET networks. However, the ubiquitous use of TCP and IP protocols makes it difficult to reach a consensus on another stack, particularly as the applications for VANETs have not been very clearly defined yet.

Security

Security is very important in VANETs. VANETs must satisfy several strict requirements before they can be deployed. These requirements include user and data authentication, privacy, liability, and secure communication. Satisfying these requirements in highly dynamic and mobile VANETs is a difficult problem but one that is particularly important because a compromised VANET could result in the loss of human life.

Security Issues in VANETs

Authentication is an extremely important property for the proper operation of VANETs. For example, an attacker could inject false information into the network by announcing a non-existent traffic jam or a false accident report. A false traffic jam announcement could cause traffic to be diverted from one road to another and actually cause a traffic jam. A false accident announcement could cause emergency braking and potentially result in real accidents. Similarly, denial-of-service attacks and masquerading attacks also can be envisioned.

[15] *e.g., small (safety) packets generated at a high rate must be signed and then authenticated.*

Even though user and data authentication was extensively studied in wired and wireless networks, the special requirements of VANETs[15] make this task more difficult.

It is understandable that if, on the one hand, authentication is a mandatory property in a VANET, then, on the other hand, privacy is also a desirable property. Privacy is a major issue in VANETs because tracking vehicles would be easy and cost effective unless proper steps are taken. Attackers could install a network of cheap radio transceivers to eavesdrop on all wireless communication in the VANET. The larger the number of transceivers, the greater the strength. Then, vehicles could be linked to the actual identity of the person by tracking the movement pattern from home to workplace. The dangers could be as annoying as targeted advertisements or as sinister as surveillance. Privacy also could be compromised due to the identifiers used in networking protocol stacks. If these identifiers (e.g., MAC and IP addresses, etc.) are never changed, they could be linked to the vehicles. Usually, VANET applications also require the information to be very accurate, for example, location information in safety applications. This information could be used by attackers to gather personal information about the users, for example, their location and movement patterns.

Liability is an extremely important requirement in a VANET and is closely related to authentication. For instance, the police or other government authorities might need to know the identity of a particular vehicle or user in certain situations, for example, an accident. However ensuring anonymity and privacy in a VANET while maintaining access control and liability is difficult. They appear to be contradictory properties, and thus, precise requirements for each of these properties must be defined, and a very careful design of security schemes must be undertaken.

Performance and real-time delivery is also an issue for security in VANETs. VANETs will have a large amount of broadcast, multicast, or traffic. In particular, safety messages are transmitted by all vehicles with a frequency between 100 ms to 300 ms. Therefore, the cryptographic techniques used in VANETs must have low traffic and processing overheads.

Another problem is the fact that possible attacks against VANETs have not been studied widely because there are no VANETs actually deployed in real-life situations. Defense against unknown attacks is somewhat difficult.

Proposed Security Schemes in VANETs

To ensure authentication, certification authorities (CAs) could be used. Currently, vehicles and their drivers are managed at regional, national, and international levels by well-defined organizations. A similar architecture could be used for CAs, each responsible for identity and credential management, as well as certification of users and vehicles in a domain. Each vehicle and road side unit (RSU) would have a unique identity, public and private keys, and a certificate. There also would be cross-certifications between CAs. This would allow local management while ensuring secure global communication. DSRC/802.11p, which is considered likely to be adopted as the communication technology in VANETs, proposes using asymmetric cryptography to sign safety messages.

Pseudonyms, which can be used to make communication anonymous, were suggested as one way of improving privacy in VANETs in [80] and others. Instead of using a long-term key pair, a node signs outgoing messages using the private key of a pseudonym and appends the pseudonym to the messages. Because messages signed under the same pseudonym can be linked together, the node should change its pseudonym periodically. Over time, linking the vehicle with the pseudonym becomes hard. Pseudonym providers could be the CAs or some other entity that issues the pseudonyms to the nodes. The change of pseudonyms must be accompanied by a change in the underlying identifiers, for example, the MAC and network addresses; otherwise the vehicle still could be tracked. However, network operations may require that these attributes do not change over a certain period of time or during a transaction. To overcome this problem, [80] suggests encrypting the end-to-end attributes, for example, IP addresses, and using the newly assigned attributes over the wireless medium.

However, changing pseudonyms in a monitored region reduces their effectiveness because the vehicle still can be tracked if the attacker easily can link the two pseudonyms used successively by the vehicle. It is best to change them in an unmonitored area or at least in a region where it is difficult to continue to track the vehicle. Freudiger *et al.* propose that this change should occur in a zone around a road intersection [81]. The success of this approach depends upon the density of vehicles and the unpredictability of their trajectories. The protocol requires that there is an RSU at the intersection. The RSU and the vehicle exchange a symmetric key as the vehicle approaches the intersection. Using this key, the vehicle obtains the new pseudonym through encrypted communication with the RSU. Thus, an attacker monitoring the intersection will not know the next pseudonym. Each intersection crossed increases the physical anonymity of the vehicle. It must be noted that because pseudonyms are bound to the long-term identity of the vehicle, it should be possible to infer it. Thus, a security architecture based on pseudonyms also could satisfy a liability property.

When certificates are used to provide authentication, the issue of certification revocation must be handled. If a vehicle must be removed from the VANET, perhaps due to some administrative problem, then the CA could issue a certificate revocation list (CRL) to the pseudonym provider. If the vehicle is using pseudonyms, this will prevent it from obtaining new pseudonyms after the current ones expire. However, it could continue to use the current pseudonyms. To counter this, compressed CRLs could be distributed over the whole VANET using the infrastructure. Alternatively, vehicles could be required to download proof of the validity of their certification from their CA. These verifiers could be included when their certificate is presented to other nodes; see [82, 83].

Another technique for the removal of a vehicle from the VANET was proposed by Raya *et al.* [84]. A vehicle detects that another vehicle is misbehaving or displaying fault symptoms. It does this by checking against a set of evaluation rules. For example, one rule might be that a packet is received beyond the sender's expected propagation distance. On detecting such a misbehaving vehicle, the vehicle transmits a warning message to surrounding neighbors. Vehicles in a particular neighborhood keep count of the number of warnings against a particular node. If the count crosses a certain threshold, they start ignoring the messages from the misbehaving vehicle. This would result in the misbehaving vehicle being temporarily evicted from the VANET. However, if enough evidence were gathered against a particular vehicle, the CA could revoke its certificates and keys. The assumption here, of course, is that the majority of vehicles are honest.

Trusted components (TC) or tamperproof devices (TPD) are mandatory to avoid attacks by fake messages that could announce false information, as shown in [80, 81]. This tamper-resistant hardware and firmware must store sensitive cryptographic material and perform cryptographic operations. A TC must have a CPU and memory to encrypt, decrypt, and so on; non-volatile memory to store keys, certificates, and so on; a real-time clock and battery to ensure the freshness of the

encrypted messages; and also must guard against certain cryptographic attacks. Positioning systems and other sensors also can be part of the TC. The TC also can be used to remove the vehicle from the VANET. The CA could directly communicate with the TC to erase all cryptographic material and cease to function.

Confidentiality for unicast traffic could be achieved by exchanging a symmetric key between vehicles through public key cryptography (see [80]).

Lessons Learned

Security in VANETs is a recent topic; most studies on the subject were published only in the last few years. This subject adds new problems, for example, privacy and anonymity, detection of compromised vehicles, and so on. Probably the most noticeable aspect concerning security in VANETs is the requirement for somewhat contradictory properties, such as authentication and liability versus privacy and anonymity, and robustness of cryptographic algorithms versus real-time requirements of cryptographic schemes. Although a few papers present rather convincing general security architectures, there is still a lack of precise specifications for a real security system and consequently, a lack of performance evaluation. Such a step is necessary to assess whether the specified system is capable of satisfying the rather contradictory properties that are desirable in VANETs.

Simulation

Simulation of VANETs is an interesting area. Most research in ad hoc networks was performed using the random waypoint model. However, objections to using this model for VANETs arise because of the restricted nature of vehicle movement. According to Saha and Johnson in [85], the random waypoint model is, in fact, an acceptable approximation of vehicle movement, and therefore, it can be used for the initial development of an application or a routing protocol. Nevertheless, for advanced design, when a more accurate matching between simulation and real life is required, a dedicated vehicular traffic simulator will be required. Therefore, for VANET research, a realistic vehicular traffic simulator is required that also can perform realistic wireless network simulations.

The normal approach is that a vehicular traffic simulator is used to generate an output, for example, trace files, which then can be used as input for a network simulator. Saha and Johnson use this approach in [85]. Their tool utilizes road maps from the U.S. Census Bureau to generate network simulator (ns)-2 scenarios [86]. Ns-2 is a popular network simulator in ad hoc research circles. Nodes start at a random point on a road and move toward another random point located on another random road. Füßler *et al.* also present a similar tool in [87], which not only generates movement files suitable for ns-2, but also provides visualization and evaluation. Lee and Wong [88] use MIcroscopic Traffic SIMulator (MITSIM) [89] with ns-2. MITSIM has the advantage of producing relatively realistic vehicular traffic movement because it uses real-life traffic control data, as well as routing information from traffic management systems. Karnadi, Mo, and Lan [90] presented a mobility model generator that can generate trace files that are usable with ns-2 and QualNet [91], another popular network simulator. The University of Southern California (USC) mobility generator tool contains a set of mobility scenario generators compatible with ns-2. Fujimoto, Wu, and Riley in [92] and Yin *et al.* in [93] use the corridor simulation model (CORSIM) [94] as the microscopic transportation simulator and QualNet as the network simulator. Mahajan *et al.* [95] developed their own mobility models as part of C++ programs that could generate ns-2 compatible pattern files.

Another approach to VANET simulation is to integrate the vehicular traffic mobility model in the network simulator, either as an extension or as an integral part. The advantage of this approach is that it could test those applications that provide information to the vehicles and expect an action based on that information. One example is a congestion-avoidance application that alters the route of the vehicle to avoid congested areas. Choffnes and Bustamante adopt this approach when they present STreet RAndom Waypoint (STRAW) in [96]. Schroth *et al.* [97] have coupled ns-2 with CARSIMA through a TCP connection enabling them to exchange the geographic position of vehicles and changes in routes, and so on. CARSIMA is a proprietary BMW vehicular traffic simulator that is not available for downloading.

Lessons Learned

Several scenario generators are available for ns-2 and QualNet. An attempt also was made to couple traffic and network simulators. However, to simulate large-scale road networks for realistic user and safety applications, an integrated simulator would be vital. Special simulators also are required to correctly simulate accidents, so as to evaluate safety applications. These micro simulators must simulate only a small portion of the road with a small number of cars, but the vehicle movements, driver reactions, and so on, should be very accurate. These could be coded from scratch or developed as an extension of ns-2. Another point to note is that currently, most network simulators use the 802.11 technology as the default. It would be interesting to incorporate other proposed technical solutions into the simulators to make realistic comparisons.

Related Projects or Organizations

In this section we briefly review related projects or organizations that are working in the field of VANETs.

European Projects

The European Commission (EC) launched several projects to increase road safety and decrease the number of road fatalities. All of these projects are actively involved in vehicle communication and VANETs.

One of these, the eSafety Forum [98], enables public sector entities from all European Union (EU) countries and the automobile industry to work closely together. Its working groups cover all relevant areas of intelligent vehicle safety systems. The European project COMeSafety is concerned especially with the V2V and V2I communication aspects of such a system.

SAFESPOT [3] is another EC-funded project that is developing a driver assistance program. An "assistant" will reduce road accidents by providing drivers with advance warning about potential dangers. SAFESPOT will use V2I and V2V communication in a cooperative manner to increase a driver's situational awareness.

The European Project CarTALK 2000 [99] focused on using V2V communication to develop a driver assistance system. It was composed of representatives from the car and communication industry, as well as research institutes.

The Cooperative Vehicle-Infrastructure Systems (CVIS) is a European project aiming to develop technologies to allow continuous V2V and V2I communication, as well as an open architecture for cooperative applications and services.

The integrated EU project, CO-OPERative networks for intelligent road Safety (COOPERS) [100] focuses on providing safety information to vehicles using infrastructure to vehicle (I2V) communication. The project is developing an architecture, new standards, new applications, and VANET-specific protocols that will be part of a cooperative traffic management solution.

The main objective of FleetNet [11] is to develop a platform for V2V communication systems. The basic approach to achieve this goal is to investigate mobile ad hoc radio networks. This approach leads to a number of technical challenges in various fields of radio hardware, radio protocols, and Internet protocols.

The Secure Vehicular Communication (SeVeCOM) [101] project is an EU-funded project working on defining security requirements and architecture in VANETs, as well as the implementation of a VANET-specific security solution.

Global System for Telematics (GST) [102] is an EU-funded integrated project focusing on providing innovative and inexpensive telematics services to manufacturers and consumers. It includes several sub-projects dealing with various topics, for example, safety channels, security, and so on.

The PReVENT PReVENTive and Active Safety Applications(PReVENT) is a combined EC and private industry project. The main idea is to develop safety applications and technologies that avoid or mitigate accidents. These will take the driver's state, as well as the nature of the danger, into account.

National Projects

Network on Wheels (NoW) [103] is a German research project that works in close collaboration with the C2C-CC [49]. Its main interest is the development of communication protocols and security for V2V communication. It is working on a testbed for functional tests and demonstrations.

The Partners for Advanced Transit and Highways (PATH) program [104] is a collection of research projects funded by the U.S. government and private industry. These projects cover a range of topics spread over several universities. The topics of interest include research in policy and behavioral aspects, transportation safety, traffic operations, and transit operations.

The U.S. Department of Transportation (DoT) Intelligent Transportation Systems (ITS) program [105] focuses on developing an intelligent transportation system using V2I and V2V communication. It has nine major initiatives covering all the major areas of such a system.

Organizations

The C2C-CC [49] is a non-profit organization established by major European car manufacturers, for example, Audi, BMW, Volkswagen, Renault, Opel, Honda, Fiat, and Daimler-Chrysler, that interacts with research centers. Its main purpose is to increase road safety using V2V communication. The C2C-CC also works on standardization in this field for the European region.

As mentioned in the previous sections, the IEEE organization hosts the standardization of the wireless access in vehicular environments (WAVE, IEEE P1609 standard family). The IEEE organization also is in charge of the IEEE 802.11p standard.[16]

[16] *IEEE 802.11p is actually a part of the IEEE P1609 standard family.*

Conclusion

VANETs are a specialized form of MANETs with specific requirements. In this article, we summarized the problems involved in developing applications for VANETs and looked at studies that were performed in this area. This domain is recent; the oldest contributions are less than ten years old, and most of the contributions were made over the last five years. There are a number of contributions that produced significant results, but the general feeling is that the subject still is not mature, and that a lot of work remains to be done.

At the PHY/MAC level, there is a domination of random-access techniques and, more precisely, the IEEE 802.11 DCF scheme. The number of proposed alternatives remains small, and there is a lack of understanding of what could be the best access protocol when both time and space are shared. It can be noted that the MAC scheme for VANETs must cope with a great variation in vehicle density over the network, and this problem was not encountered in wired and even in the usual wireless local area networks.

Concerning the routing issue, geographic routing may be considered as the right approach for VANETs, but as yet, there have been no convincing studies to prove that such an approach outperforms classical routing schemes. Even if the impact of mobility is beginning to be understood, there remains a profound lack of consideration of realistic radio propagation models to design efficient routing protocols.

The TCP/IP stack obviously is not well adapted to VANETs, and there is a lot of research to be done in this area, even though a few interesting results exist already. However, the momentum of TCP/IP is such that one might wonder whether changing this widely accepted stack for a new approach is realistic in the near future. More probably, there will be an adaptation and improvement of TCP/IP for VANETs.

A special need also exists for techniques to disseminate information in VANETs, and it is not clear whether these techniques must be implemented at the MAC layer, the routing layer, or in the application itself.

The challenge of security is very important for VANETs. Although the problems are starting to be clearly identified and initial security architectures are starting to be proposed, a great deal of work remains to be done in this area to ensure that the rather contradictory security requirements of VANETs can be satisfied.

The studies that we reviewed in this article usually try to solve only one specific problem. They never try to propose a general architecture for VANETs or to solve the issues raised by VANET safety applications and by VANET user applications simultaneously. Solving such an "equation" is probably the key to building successful VANETs. The solution to all of these issues probably requires integrating smart mechanisms into more than one layer.

This presentation followed the open system interconnection (OSI) reference model. However, this model probably is less relevant for VANETs than for conventional networks because it was designed for conventional wired networks and, as we have seen, issues in VANETs are significantly different from those in conventional networks. This reinforces the idea that solving issues for VANETs likely requires a cross-layer approach.

References

[1] S. Corson and J. Macker, "Mobile Ad Hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations," RFC editor, 1999.

[2] "COMESAFETY," www.comesafety.org

[3] "SAFESPOT," www.safespot-eu.org
[4] "European project PReVENT-Intersafe," http://www.prevent-ip.org/en/prevent_subprojects/intersection_safety/intersafe
[5] O. Dousse, P. Thiran, and M. Hasler, "Connectivity in Ad-Hoc and Hybrid Networks," *Proc. IEEE INFOCOM 2002 21st Annual Joint Conf. IEEE Computer and Communications Societies*, vol. 2, 2002.
[6] C. D. Wang and J. P. Thompson, "Apparatus and Method for Motion Detection and Tracking of Objects in a Region for Collision Avoidance Utilizing a Real-Time Adaptive Probabilistic Neural Network," U.S. patent no. 5,613,039, 1997.
[7] B. Mourllion, "Extension d'un Systéme de Perception Embarqué Par Communication, Application é la Diminution du Risque Routier," Ph.D. diss., Université Paris 11 (Orsay), 2006.
[8] "U.S. Department of Transportation," http://safety.fhwa.dot.gov/facts/road factsheet.htm
[9] "European project REACT," www.react-project.org
[10] J. Gluck, H. S. Levinson, and V. Stover, "Impacts of Access Management Techniques," NCHRP Report 420, Transportation Research Board, 1999; http://tools.ietf.org/wg/manet/draft-ietf-manet-zone-zrp/draft-ietf-manet-zone-zrp-04.txt
[11] H. Hartenstein *et al.*, "Position-Aware Ad Hoc Wireless Networks for Inter-Vehicle Communications: The FleetNet Project," *MobiHoc '01: Proc. 2nd ACM Int'l. Symp. Mobile Ad Hoc Networking & Computing*, New York: ACM Press, 2001, pp. 259–62.
[12] A. Ueda, K. Mizui, and T. Ihara, "Intervehicle Communication and Ranging System Using Code-Hopping Spread Spectrum Technique," *Electronics and Communications in Japan*, pt. 3, vol. 88, no. 5, 2005.
[13] M. Haardt, "TD-CDMA Based on UTRA TDD Mode," *IEEE JSAC*, vol. 18, no. 8, 2000, pp. 1375–85.
[14] A. Ebner *et al.*, "Performance of UTRA TDD Ad Hoc and IEEE 802.11b in Vehicular Environments," *IEEE 57th Vehic. Tech. Conf. Spring 2003*, vol. 2, 2003, pp. 960–64.
[15] D. Dhoutaut, A. Regis, and F. Spies, "Impact of Radio Propagation Models in Vehicular Ad Hoc Networks Simulations," *ACM Int'l. Wksp. Vehic. Ad Hoc Networks (VANETs)*, 2006.
[16] D. Dhoutaut and F. Spies, "Adding Geographical Interferences into the Shadowing Pattern Model for Vehicular Ad Hoc Networks Simulations," *Proc. 7th Int'l. Conf. Intelligent Transport Systems*, 2007, pp. 105–10.
[17] J. Hartwell and A. Fapojuwo, "Modeling and Characterization of Frame Loss Process in IEEE 802.11 Wireless Local Area Networks," *IEEE 60th Vehic. Tech. Conf. Fall 2004,* vol. 6, 2004, pp. 4481–85.
[18] N. Abramson, "The Aloha System — Another Alternative for Computer Communication," *AFIPS*, 1970, pp. 295–98.
[19] L. Kleinrock and F. A. Tobagi, "Packet Switching in Radio Channels: pt. 1: Carrier-Sense Multiple-Access Modes and Their Throughput-Delay Characteristics," *IEEE Trans. Commun.*, vol. COM–3, 1975, pp. 1400–16.
[20] D. Bertsekas and R. Gallager, *Data Networks*, Prentice-Hall, 2001.
[21] P. Karn, "MACA — A New Channel Access Method for Packet Radio," *ARRL/CRRL Amateur Radio 9th Computer Networking Conf.*, ARRL, 1990, pp. 134–40.
[22] "Dedicated Short Range Communications (DSRC)," http://www.leearmstrong.com/dsrc/dsrchomeset.htm
[23] J. Singh *et al.*, "Wireless LAN Performance under Varied Stress Conditions in Vehicular Traffic Scenarios," *IEEE 56th Vehic. Tech. Conf. Fall 2002*, vol. 2, 2002, pp. 743–47.
[24] F. Borgonovo *et al.*, "RR-Aloha, a Reliable R-Aloha Broadcast Channel for Ad-Hoc Inter-Vehicle Communication Networks," *Med-Hoc-Net 2002*, Baia Chia, Italy, 2002; citeseer.ist.psu.edu/borgonovo02rraloha.html
[25] W. Crowther *et al.*, "A System for Broadcast Communication: Reservation-ALOHA," *Proc. 6th Hawaii Int'l. Conf. Systems Sciences*, 1973, pp. 596–603.
[26] D. Lee *et al.*, "A Wireless Token Ring Protocol for Ad-Hoc Networks," *Proc. IEEE Intelligent Transportation System Conference (ITSC'01)*, 2001.
[27] P. Gupta and P. R. Kumar, "The Capacity of Wireless Networks," *IEEE Trans. Info. Theory*, vol. 46, no. 2, 2000, pp. 388–404.
[28] F. Baccelli, B. Blaszczyszyn, and P. Mühlethaler, "An Aloha Protocol for Multihop Mobile Wireless Networks," *IEEE Trans. Info. Theory*, vol. 52, no. 2, 2006, pp. 421–36.
[29] J. Blum, "Adaptive Space Division Multiplexing: An Improved Link Layer Protocol for Inter-Vehicle Communication," *IEEE Int'l. Conf. WiMob 2005*, vol. 3, 2005, pp. 22–24.
[30] K. Dobashi, "Adaptive MAC Protocol for High-Load Inter-Vehicle Communication," *Wireless and Mobile Computing, Networking and Commun. Mag.*, vol. 44, no. 1, 2006, pp. 74–82.
[31] S. Yi, Y. Pei, and S. Kalyanaraman, "On the Capacity Improvement of Ad Hoc Wireless Networks Using Directional Antennas," *MobiHoc '03: Proc. 4th ACM Int'l. Symp. Mobile Ad Hoc Networking & Computing*, ACM Press, 2003, pp. 108–16.
[32] M. Sadashivaiah, "Adaptive MAC Protocol for High-Load Inter-Vehicle Communication," *IEEE 61st Vehic. Tech. Conf. Spring 2005*, vol. 4, 2005.
[33] L. Liu *et al.*, "A Vehicle-to-Vehicle Communication Protocol for Cooperative Collision Warning," *1st Annual Int'l. Conf. Mobile and Ubiquitous Systems: Networking and Services, MOBIQUITOUS 2004*.
[34] M. Torrent-Moreno, P. Santi, and H. Hartenstein, "Fair Sharing of Bandwidth in VANETs," *Vehicular Ad Hoc Networks*, 2005.
[35] C. Liu and J. Kaiser, "A Survey of Mobile Ad Hoc Network Routing Protocols," Ulm University, Report Series Nr. 2003-08, 2003.
[36] M. Grossglauer and D. N. C. Tse, "Mobility Increases the Capacity of Ad Hoc Wireless Networks," *IEEE/ACM Trans. Net.*, vol. 10, no. 4, 2002, pp. 477–86.
[37] T. Clausen *et al.*, "Optimized Link State Routing Protocol (OLSR)," RFC 3626, Oct. 2003, Network Working Group; http://ietf.org/rfc/rfc3626.txt
[38] C. Perkins, E. Belding-Royer, and S. Das, "Ad Hoc On-Demand Distance Vector (AODV) Routing," RFC 3561, 2003, Network Working Group; www.ietf.org/rfc/rfc3561.txt
[39] D. B. Johnson, D. A. Maltz, and Y.-C. Hu, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)," 2004; http://www.ietf.org/internet-drafts/draft-ietf-manet-dsr-10.txt
[40] C. S. R. Murthy and B. Manoj, *Ad Hoc Wireless Networks: Architectures and Protocols*, Prentice Hall PTR, 2004.
[41] C. E. Perkins, *Ad Hoc Networking*, Addison-Wesley Professional, 2001.
[42] L. Viennot, P. Jacquet, and T. Clausen, "Analyzing Control Traffic Overhead Versus Mobility and Data Traffic Activity in Mobile Ad-Hoc Network Protocols," *Wireless Networks*, vol. 10, no. 4, 2004, pp. 447–55.
[43] B. Karp, "Geographic Routing for Wireless Networks," Harvard University, Ph.D. diss., 2000; citeseer.nj.nec.com/karp00geographic.html
[44] S. Basagni, I. Chlamtac, and V. S. Highway Traffic Safety, "Geographic Messaging in Wireless Ad Hoc Networks," *IEEE 49th Vehic. Tech. Conf.*, 1999, vol. 3, 1999, pp. 1957–61.
[45] G. G. Finn, "Routing and Addressing Problems in Large Metropolitan-Scale Internetworks," IST Res. Rep. ISU/RR 87–80, 1987.
[46] X. Lin and I. Stojmenovic, "Loop-Free Hybrid Single-Path/Flooding Routing Algorithms with Guaranteed Delivery for Wireless Networks," *IEEE Trans. Parallel and Distributed Systems*, vol. 12, 2001, pp. 1023–32.
[47] I. Stojmenovic and X. Lin, "Power-Aware Localized Routing in Wireless Networks," *IEEE Trans. Parallel and Distributed Systems*, vol. 12, no. 11, 2001, pp. 1122–33.
[48] M. Mauve, J. Widmer, and H. Hartenstein, "A Survey on Position-Based Routing in Mobile Ad Hoc Networks," *IEEE Network Mag.*, vol. 15, no. 6, Nov. 2001, citeseer.ist.psu.edu/article/mauve01survey.html, pp. 30–39.
[49] "Car 2 Car," http://www.car-to-car.org
[50] B. Ducourthial, Y. Khaled, and M. Shawky, "Conditional Transmissions: A Strategy for Highly Dynamic Vehicular Ad Hoc Networks," Heudiasyc lab. UMR CNRS 6599, Université de Technologie de Compiégne, Tech. Rep., 2006.
[51] K. Wu and J. Harms, "Performance Study of Proactive Flow Handoff for Mobile Ad Hoc Networks," *Wireless Networks*, vol.

12, no. 1, 2006, pp. 119–35.
[52] H. Menouar, M. Lenardi, and F. Filali, "Improving Proactive Routing in VANETs with the MOPR Movement Prediction Framework," *Proc. 7th Int'l. Conf. Intelligent Transport Systems*, 2007, pp. 438–43.
[53] H. Wu, R. Fujimoto, R. Guensler, and M. Hunter, "MDDV: A Mobility-Centric Data Dissemination Algorithm for Vehicular Networks," *Vehicular Ad Hoc Networks*, 2004.
[54] T. Nadeem, P. Shankar, and L. Iftode, "A Comparative Study of Data Dissemination Models for VANETs," *3rd ACM/IEEE Annual Int'l. Conf. Mobile and Ubiquitous Systems: Networks and Services (MOBIQUITOUS 2006)*, July 17–21, 2006, San Jose, California.
[55] M. M. B. Tariq, M. H. Ammar, and E. W. Zegura, "Message Ferry Route Design for Sparse Ad Hoc Networks with Mobile Nodes," *MobiHoc*, 2006, pp. 37–48.
[56] D. Kutscher and J. Ott, "The 'Drive-Thru' Architecture: WLAN-Based Internet Access on the Road," *IEEE 59th Vehic. Tech. Conf. Spring 2004*, vol. 5, pp. 2615–22.
[57] V. Namboodiri, M. Agarwal, and L. Gao, "A Study on the Feasibility of Mobile Gateways for Vehicular Ad-Hoc Networks," *Proc. VANET'04*, 2004.
[58] V. Devarapalli *et al.*, "Network Mobility (NEMO)," RFC 3963, Jan. 2005; http://ietf.org/rfc/rfc3963.txt
[59] T. Ernst, "The Information Technology Era of the Vehicular Industry," *SIGCOMM Comput. Commun. Rev.*, vol. 36, no. 2, 2006, pp. 49–52.
[60] R. Wakikawa *et al.*, "Design of Vehicle Network: Mobile Gateway for MANET and NEMO Converged Communication," *Proc. 2nd ACM Int'l. Wksp. Vehicular Ad Hoc Networks*, ACM Press, 2005, pp. 81–82.
[61] E. Pagani and G. P. Rossi, "Call Admission Multicast Protocol (CAMP) for End-to-End Quality-of-Service," citeseer.ist.psu.edu/473829.html
[62] S. Bae, S. Lee, and M. Gerla, "Unicast Performance Analysis of the ODMRP in a Mobile Ad Hoc Network Testbed," *Proc. IEEE Int'l. Conf. Commun. and Networks (ICCCN)*, Las Vegas, Oct. 2000, citeseer.ist.psu.edu/bae00unicast.html
[63] E. Royer and C. Perkins, "Multicast Ad Hoc On-Demand Distance Vector (MAODV) Routing," IETF, Internet draft: draft-ietf-manet-maodv-00.txt, 2000, citeseer.ist.psu.edu/royer00multicast.html
[64] P. Jacquet *et al.*, "Multicast Optimized Link State Routing," Nov. 2001, Internet draft: draft-ietf-manet-olsr-molsr-01.txt
[65] S. Biswas, F. Dion, and R. Tatchikou, "Vehicle-to-Vehicle Wireless Communication Protocols for Enhancing Highway Traffic Safety," *IEEE Commun. Mag.*, vol. 44, 2006, pp. 74–82.
[66] A. Laouiti, P. Mühlethaler, and Y. Toor, "Comparison of Flooding Techniques for Safety Applications in VANETs," *Proc. 7th Int'l. Conf. Intelligent Transport Systems*, 2007, pp. 444–49.
[67] J. Bransted and L. M. Kristensen, "Specification and Performance Evaluation of Two Zone Dissemination Protocols for Vehicular Ad-Hoc Networks," anss, vol. 0, 2006, pp. 68–79.
[68] R. Fracchia, "Knowing Vehicles Location Helps Avoiding Broadcast Packets Storm," *PerCOMW*, vol. 0, 2006, pp. 118–23.
[69] S. Ghandeharizade, S. Kapadia, and B. Krishnamachari, "PAVAN: A Policy Framework for Content Availability in Vehicular Ad-Hoc," *Vehic. Ad Hoc Networks*, 2004.
[70] T. Repantis and V. Kalogeraki, "Data Dissemination in Mobile Peer-to-Peer Networks," *Mobile Data Management*, 2005.
[71] S. Xu and T. Saadawi, "Does the IEEE 802.11 MAC Protocol Work Well in Multihop Wireless Ad Hoc Networks?" *IEEE Commun. Mag.*, vol. 39, no. 6, 2001, pp. 130–37.
[72] T. Nandagopal *et al.*, "Achieving MAC Layer Fairness in Wireless Packet Networks," Mobile Computing and Networking, 2000, citeseer.ist.psu.edu/nandagopal00achieving.html, pp. 87–98.
[73] T. Ozugur, M. Naghshineh, P. Kermani, and J. Copeland, "Fair Media Access for Wireless LANs," *Proc. IEEE GLOBECOM '99*, citeseer.ist.psu.edu/ozugur99fair.html
[74] Revealing TCP Unfairness Behavior in 802.11 Based Wireless Multi-Hop Networks, vol. 2, 2001.
[75] K. Chandran *et al.*, "A Feedback Based Scheme for Improving TCP Performance in Ad-Hoc Wireless Networks," *IEEE Pers. Commun.*, Feb. 2001, pp. 34–39.
[76] G. Holland and N. H. Vaidya, "Analysis of TCP Performance over Mobile Ad Hoc Networks," *Mobile Computing and Networking*, 1999, citeseer.ist.psu.edu/holland99analysis.html, pp. 219–30.
[77] D. Kim, C.-K. Toh, and Y. Choi, "TCP-Bus: Improving TCP Performance in Wireless Ad-Hoc Networks," *J. Commun. and Networks*, vol. 3, 2001, pp. 1–12.
[78] S. Kopparty *et al.*, "Split TCP for Mobile Ad Hoc Networks," *IEEE Global Telecommun. Conf., 2002,* vol. 1, 2002, pp. 138–42.
[79] "Control-Based Mobile Ad-Hoc Networking Program," 2005; http://www.darpa.mil/sto/solicitations/CBMANET
[80] P. Papadimitratos *et al.*, "Architecture for Secure and Private Vehicular Communications," *Proc. 7th Int'l. Conf. Intelligent Transport Systems*, 2007, pp. 339–34.
[81] J. Freudiger *et al.*, "Mix-Zones for Location Privacy in Vehicular Networks," *WiN-ITS*, 2007.
[82] S. Miscali, "Efficient Certificate Revocation, MIT Laboratory for Computer Science, " Tech. Rep. TM-542b, Mar. 1996, Tech. Rep.
[83] F. Kargl, S. Schlott, and M. Weber, "Identification in Ad Hoc Networks," *HICSS '06: Proc. 39th Annual Hawaii Int'l. Conf. System Sciences*, Washington, DC: IEEE Computer Society, 2006, p. 233c.
[84] M. Raya *et al.*, "Eviction of Misbehaving and Faulty Nodes in Vehicular Networks," *IEEE JSAC*, special issue on Vehicular Networks, 2007.
[85] A. K. Saha and D. B. Johnson, "Modeling Mobility for Vehicular Ad-Hoc Networks," *Vehicular Ad Hoc Networks*, 2004.
[86] "The network simulator-ns," http://www.isi.edu/nsnam/ns/
[87] H. Füßler *et al.*, "Studying Vehicle Movements on Highways and Their Impact on Ad-Hoc Connectivity," Technical Report TR–005-003, Dept. of Math. and C.S., Univ. of Mannheim, 2005.
[88] A. Lee and K. D. Wong, "Comparison of On-Demand Ad-Hoc Routing Protocols in a Vehicular Ad-Hoc Network Environment," *MMU Int'l. Symp. Information and Communications Technologies (M2USIC)*, Malaysia, 2005.
[89] "MIcroscopic Traffic SIMulator (MITSIM)," http://mit.edu/its/mitsimlab.html
[90] F. K. Karnadi, Z. H. Mo, and K.-C. Lan, "Rapid Generation of Realistic Mobility Models for VANET," under submission.
[91] "QualNet Network Simulation Software," http://www.qualnet.com/
[92] R. Fujimoto, H. Wu, and G. Riley, "Analytical Models for Information Propagation in Vehicle-to-Vehicle Networks," *IEEE 60th Vehic. Tech. Conf.*, Fall 2004, vol. 6.
[93] J. Yin *et al.*, "Performance Evaluation of Safety Applications over DSRC Vehicular Ad Hoc Networks," *Proc. VANET*, Oct. 2004, citeseer.ist.psu.edu/article/yin04performance.html
[94] "CORridor SIMulation (CORSIM) Vehicle Traffic Simulator," http://ops.fhwa.dot.gov/trafficanalysistools/corsim.htm
[95] A. Mahajan *et al.*, "Evaluation of Mobility Models for Vehicular Ad-Hoc Network Simulations," Technical Report TR-051220, Department of Computer Science, Florida State University, 2005.
[96] D. R. Choffnes and F. E. Bustamante, "An Integrated Mobility and Traffic Model for Vehicular Wireless Networks," *VANET '05, Proc. 2nd ACM Int'l. Wksp. Vehicular Ad Hoc Networks*, ACM Press, 2005, pp. 69–78.
[97] C. Schroth *et al.*, "Simulating the Traffic Effects of Vehicle-to-Vehicle Messaging Systems," *5th Int'l. Conf. ITS Telecommunications (ITS-T)*, 2005.
[98] "eSAFETY," www.esafetysupport.org
[99] "CarTALK," www.cartalk2000.net
[100] "COOPERS," www.coopers-ip.eu
[101] "SEVECOM," www.sevecom.org
[102] "GST," www.gstproject.org
[103] "NOW," www.network-on-wheels.de
[104] "PATH," www.path.berkeley.edu
[105] "USDoT ITS program," www.its.dot.gov

BIOGRAPHIES

ANIS LAOUITI received his Ph.D. in computer science from Versailles University, France, in 2002. He joined the GET/INT, France, as an assistant professor in 2006. He was with the INRIA/Hipercom team from 1998 to 2006. His research interests include unicast/multicast routing protocols for MANETs and vehicle-to-vehicle communications.

ARNAUD DE LA FORTELLE has a Ph.D. in applied mathematics and engineering from the French Ecole Polytechnique and Ecole des Ponts et Chauss Ã©es. He is a civil servant at the French Transport Ministry and is currently the director of the Joint Research Unit LaRA (between INRIA, Armines, and Mines Paris). He manages several French and European projects (Puvame, Prevent/Intersafe, REACT, COM2REACTž2026) for LaRA.

PAUL MÜHLETHALER (Paul.Muhlethaler@inria.fr) is a research director at INRIA. His research field is network protocols and performance evaluation. His main research interests are medium access schemes, scheduling algorithms, and routing protocols. He has worked on wireless LANs at ETSI for HiPERLAN and at IETF, in the mobile ad hoc network (MANET) group, where he is one of the co-author of the OLSR routing protocol. Two main applications of his work on mobile ad hoc networks are military and vehicular networks.

YASSER TOOR is pursuing his Ph.D. degree at INRIA Rocquencourt, France, attached to the Université Pierre et Marie Curie, France. He received his Master's degree in software engineering from the National University of Science and Technology, Pakistan, and his Bachelor's degree in telecommunications from the University of Engineering and Technology, Pakistan. His main research interest is in vehicular ad hoc networks, particularly MAC layer and routing issues.