Chapter 13

Vehicular Ad Hoc Networks: Current Issues and Future Challenges

Saleh Yousefi, Mahmood Fathy, and Saeed Bastani

Contents

13.1 Introduction to Vehicular Ad Hoc Networks

Vehicular ad hoc networks (VANETs) are a special type of mobile ad hoc networks (MANETs) where wireless-equipped vehicles form a network spontaneously while traveling along the road. Direct wireless transmission from vehicle to vehicle makes it possible to communicate even where there is no telecommunication infrastructure, such as the base stations of cellular phone systems or the access points of wireless dedicated access networks. This new way of communication has been attracting much attention in the recent years in academic and industry communities. The US Federal Communications Commission (FCC) has allocated seven 10-MHz channels in the 5.9-GHz band for dedicated short range communication (DSRC) to enhance the safety and productivity of the transportation system [1]. The FCC's DSRC ruling has permitted both safety and nonsafety (commercial) applications, provided safety is assigned priority. The IEEE has taken up working on a new standard for VANETs, which is called IEEE 802.11p [2].

The communication pattern in VANETs includes two forms: vehicle to vehicle (V2V) communications and vehicle to infrastructure (V2I) communications. The former leads to a pure MANETs, while the latter can be viewed as a hybrid network. Although VANETs can be seen as a special case of MANETs, there are several distinctive characteristics that dictate special treatment of VANETs. The most important distinctive characteristics of VANETs are as follows:

- Specific mobility patterns: As any MANET, mobility pattern has a noticeable effect on the behavior and performance of the network. In the context of MANETs, many mobility patterns are proposed. However, almost none of the previous mobility models can be applied to VANETs mostly due to distinctive mobility pattern of vehicles on roads. On the one hand, the mobility pattern of VANETs is one-dimensional or stripelike. On the other hand, the mobility of vehicles is affected by sophisticated interactions between individual vehicles. The optimistic point here is that there is very rich literature in the field of transportation engineering about modeling mobility patterns. Furthermore, there are many good common traffic simulators that can be of advantage in VANET simulation. Indeed, the current trend in VANET simulation is to find ways for exploiting analytical and simulation tools of transportation engineering in the simulation process of VANETs.

- Highly dynamic topology: The topology of the network is a burden of high variability mainly due to the mobility of vehicles (in particular vehicles of the opposite direction) in highway scenario and rural environments as well as traffic lights and junctions in the urban environments. Thus, the performance of protocols' application in such unstable environments may be degraded and thus needs specific treatment.
- Intermittent connectivity: Due to the reason mentioned above, vehicles may not be able to last their communication for a long time and they may encounter several pauses during the communication period. This is the main reason why many common network protocols and their applications should be tailored for VANETs to address this kind of connectivity.
- Strict quality of service (QoS) requirements: The most important motivation of VANETs is safety applications that address life safety of people (drivers and passengers). Therefore, in spite of ordinary applications, very tough QoS metrics should be guaranteed by the network. Any violation of QoS metrics may be at the expense of people's life. This issue necessitates new performance evaluation metrics as well as protocol design techniques.

The goal of this chapter is to provide a basic knowledge about VANETs and to review state-of-the-art methods tackling the challenges as well as to present some directions for future research. To fulfill these goals, in the first four sections of this chapter, basic discussions have been presented, which are intended to give the reader a solid knowledge about VANETs and their applications and challenges. Then in the remainder of the chapter some important and advanced topics have been selected. In each case, we first state the problem in hand and the challenges, and then some example solutions are provided; finally, some open problems are presented for future research.

13.1.1 Motivation

Each year, many people suffer from different traffic causalities around the world. This issue followed by the huge economic burden of accidents urges governments to improve the level of safety on roads. In 1970s, passive safety systems such as safety belts and airbags were introduced. Although they have decreased the severity of accidents and the number of deaths and injuries, passive safety systems have not been able to decrease the number of accidents, and therefore active safety systems, such as antilock brake systems and electronic stability program systems, have been invented. The statistics published in [3] show that the active safety systems have stopped a rising trend of accidents, but the number of accidents remains almost the same for many years. In other words, it seems that the current safety systems are no longer able to decrease the number of accidents. To tackle the aforementioned problem, many investigations have been performed in order to understand the effective factors that cause accidents. The results of studies in many countries (e.g., [4]) show that the information error has the highest impact on accidents. By the information error, we mean that either the driver receives the critical information too late or the process has failed. The key factor here is the reaction time of the driver, which is relatively high (more than 1.0 s [5]) such that he or she cannot react promptly. As a result, if we could somehow increase the information horizon of the driver such that he or she could be informed about distant events earlier, it might lead to a noticeable decrease in the number of accidents as well as the number of deaths and injuries. However, recent advances in wireless technology make the idea of "communication anytime and anywhere" more reachable. Inspired from this idea, there is a growing belief that embedding wireless radios into vehicles may be quite beneficial from safety aspects. The ultimate goal is to provide new technologies that are able to improve safety and efficiency of road transport. It should be noted that telecommunication has been invoked in intelligent transportation systems (ITSs) for many years but the previous systems are centralized and include either cellular or infrastructure-based roadside to vehicle communications [6,7].

13.2 Roads Traffic Theory Basics

In order to clarify the challenges of communication in VANETs, we invoke some basic concepts from traffic theory. From the traffic theory [5] we know that there are three macroscopic parameters—speed (km/h), density (veh/km/lane), and flow (veh/h/lane)—that describe the traffic state on a road. Over the years, many models have been proposed for speed–flow–density relationships (see [5]). Simply, these parameters are related by the so-called fundamental traffic theory equation given as

$$F = S \times D \tag{13.1}$$

where F, S, and D are the traffic flow, average speed, and traffic density, respectively. As shown in Figure 13.1, the general relationship between the above basic parameters can be studied in two different phases: First, when the density is low, the flow entering and leaving a section of the highway is the same and no queues of vehicles are forming within the section. This state holds until the density reaches a threshold called critical value. This phase is called stable-flow and is shown by the solid line in the figure. The peak of the flow–density curve is the maximum rate of flow or the capacity of the highway. Beyond this density, some breakdown locations appear on the highways, which lead to forming some queues of vehicles. This phase is called forced-flow and is shown by the dashed line in the figure. If the density increases further, the traffic reaches to the jam state where vehicles have to stop completely. In the stable-flow phase, when the density is sufficiently low, the speed of vehicles and the flow are independent and thus drivers can drive as fast as they want to. This state is called free-flow state.

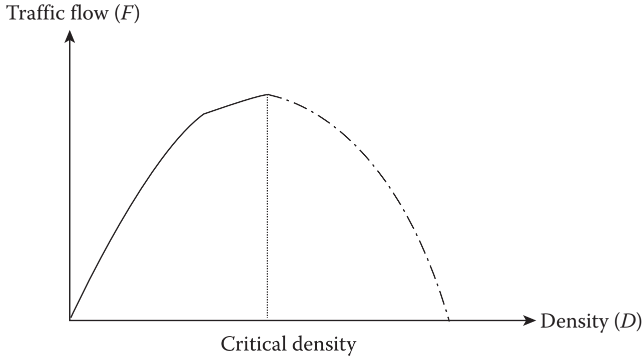


Figure 13.1 Relationship between the basic parameters in the traffic theory. (From Yousefi, S., Altman, E., El-Azouzi, R., and Fathy, M., *IEEE Trans. Veh. Technol.*, 57(6), 3341–3356, 2008. With permission. © (2008) IEEE.)

The above-mentioned traffic states determine the VANETs' challenges, which should be addressed. From the communication point of view that we peruse in VANETs, different challenges should be addressed in each traffic state. Obviously, connectivity is satisfactory in the forced-flow state while it deteriorates at light load corresponding to the free-flow state in which it might not be possible to transfer messages to other vehicles because of disconnections. However, since the network is sparse, collision between simultaneous transmissions is trivial in the free-flow state while it is one of the main communication challenges that should be addressed in the forced-flow traffic state.

13.3 VANETs' Applications and Messages

According to the FCC frequency allocation, one can categorize applications of VANETs into two main classes. The first class aims to improve the safety level in roads, i.e., safety applications. In this case, VANETs can be seen as a complementary to the current ITSs [6,7] in order to enhance the coverage and performance. The second class of applications, which is predicted to grow very fast in the near future, is commercial services, i.e., comfort applications.

13.3.1 Safety Applications

In safety applications, the goal is to improve the life safety level of passengers by exchanging safety relevant information between vehicles. The information is either presented to the driver or used by the automatic active safety system. Some examples are cooperative forward collision warning, left/right turn assistant, lane changing warning, stop sign movement assistant, and road-condition warning. Due to the stringent delay requirements, applications of this class may demand direct vehicle-to-vehicle communication.

With respect to QoS requirements, these applications are characterized by being delay and loss *intolerant*. In safety applications, usually data should be disseminated to a set of candidate vehicles; thus, broadcast (in its special form) is the dominant pattern of data dissemination. In VANETs' terminology this type of data dissemination is sometimes called geocast or roadcast, aiming at concentrating on the fact that the candidate vehicles are limited to a geographical area and/or a specific part of a road.

In the last decade, much effort has been devoted to substantiate VANETs in the real world. These efforts have brought together industrial and academic bodies in order to realize the idea. Some most important projects in this area include COMeSAFETY [8], COM2REACT [9], COOPERS [10], CVIS [11], and CICAS [12].

Any safety application demands exchange of related messages between vehicles. These massages can be classified into two categories: alarm and beacon, which have different dissemination policies and roles in safety improvement. In the following subsections, we provide a more detailed explanation.

13.3.1.1 Alarm-Based and Beacon-Based Safety Applications

Alarm messages are issued by all vehicles to announce to other vehicles about the previously happened events at a specific location of a road, such as car crash and icy surface, while beacon messages are issued periodically. Using the received beacons, vehicles try to inhibit possible events (not previously occurred) such as erroneous lane changing, forward collisions, and wrong left/right turning.

Besides, beacon messages might be used by other applications (e.g., routing protocols). Note that messages mentioned above are complementary to each other. While alarm messages may be able to inform the driver in time about already happened events in order to prevent more incidents, beacon messages can prevent many incidents before they take place. Moreover, since alarm messages announce events, they are more critical and should be disseminated with a higher priority.

13.3.2 Comfort Applications

In comfort applications, the goal is to improve passenger comfort and traffic efficiency. Examples for this category are traffic-information system, route optimization (navigation), electronic toll collection, map download, video download, and Internet on the roads. These applications are predicted to grow very fast in the near future due to business motivations. Although some of the projects introduced in Section 13.3.1 also have some subtasks related to comfort applications, one may name NOW [13] as a project focusing on data (Internet) access on roads using V2V and V2I techniques.

In this category of applications, both unicast and broadcast communications are justifiable. On the one hand, legacy data applications (e.g., FTP and HTTP) mostly require unicast communications, and on the other hand, many other applications such as map download demand broadcasting of data to all or a subclass of vehicles. Geocast or roadcast is sometimes defined as broadcasting data to a specific geographical location or to a part of the road.

13.4 Performance Evaluation Metrics for VANETs

Due to their QoS requirements, the treatment of comfort applications is similar to that of common networking applications; however, safety applications require a different treatment as explained in the following. In order to deploy safety applications in VANETs, there should be effective ways to evaluate their degree of success in providing safety. For this purpose, inspired from networking literature, researchers utilize common evaluation metrics such as delivery rate and delay. Although these metrics are also valuable for evaluating the performance of safety applications, the following distinctive characteristics necessitate specific treatment of the performance evaluation of safety applications:

- In safety applications, the lack of fresh information makes each individual vehicle a life threat for the others. Thus, in order to evaluate the performance of a message dissemination protocol or a safety application, the quality of the safety offered to all individual vehicles is critical and should be monitored. While in ordinary networking scenarios, the average values of the metrics of interest are usually evaluated, and in safety scenarios, the average values are no longer useful. Therefore, we propose to monitor the metrics of interest for all vehicles and count on the *worst-case* values.
- Although the distance (in meters) between senders and receivers may be important in some networking scenarios (e.g., sensor networks), from the safety viewpoint it is the most important metric of performance. To have a solid evaluation in safety scenarios, the coverage property need to be evaluated. In other words, for any given vehicle the range in which the safety applications can provide adequate safety is of ultimate importance. Within this range, vehicles can receive the safety messages of the initiator vehicles with a satisfactory QoS level, i.e., desirable values for delay, delivery rate, etc.

- The definite goal of any beacon-based safety application deployed in a given vehicle is to inform neighboring vehicles about the vehicle's own status. Hence, evaluating the fact that how well and how fairly the beacon dissemination protocols and/or safety applications are successful in this regard is indispensable from the safety viewpoint.

Note that the above concerns should be taken into account all together. With this in mind, we propose two new metrics, primarily focused on evaluating the performance in safety scenarios. It should be noted that the following metrics may be used along with other common evaluation metrics:

- Effective range: In any time step (say 1 s), the *effective range* is defined as the range within which the worst case of QoS metrics is satisfied. The satisfaction levels depend on the projected safety application. Although one may consider a different QoS metrics, as a possible way we define the effective range as the range within which (a) the minimum delivery rate is above a predefined threshold and (b) the maximum end-to-end delay is below a predefined threshold. Note that this metric has a value in each time step and the obtained values can be averaged to give an average number during the course of simulation time. This metric can be evaluated for both alarm-based and beacon-based safety applications.
- Beaconing rate: In any time step (say 1 s), for a given beacon disseminating vehicle the *beaconing rate* is defined as the average value among its worst-case delivery rates to all surrounding vehicles in its transmission range. This metric assists in knowing how well the beacons disseminating from a vehicle reach other vehicles. When we compare the value of this metric for different vehicles, it gives us valuable insights into the capability of the safety application in providing a fair safety performance to each vehicle. Note that this metric has a value in each time step and the obtained values can be averaged to give an average number during the course of simulation time. This metric is suitable for evaluation of safety of beacon-based safety applications.

13.4.1 Application Layer Performance

In Vehicle Safety Communication Project [14], 34 vehicle safety applications, enabled or enhanced by VANETs, were studied. Among them, 8 applications were identified as high priority and selected for extracting their communication requirements. These applications include both alarm-based and beacon-based safety applications. Typically, safety applications have the following communication requirements:

1. Communication ranges from 50 to 300 m (the more the better)
2. Safety message transmission interval from 20 ms to 1 s
3. Safety message size from 200 to 500 bytes
4. End-to-end delays below 150 ms

Note that DSRC is intended to support 1000 m transmission range. However, depending on the channel conditions and environmental obstacles, the practical transmission range may be less than the nominal values. It also uses the IEEE 802.11p MAC (medium access control) protocol, a variant of IEEE 802.11 protocol with Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) behavior. Therefore, it could be quite reasonable to consider single-hop dissemination as an important type of future intervehicle communication. However, in particular for alarm and

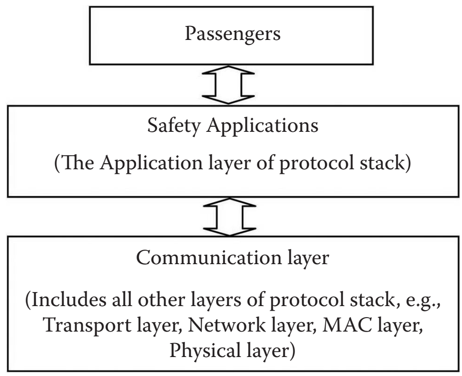


Figure 13.2 Three-layer architecture for safety applications in VANETs.

comfort messages, multihop message propagation is challenging. Note that when we focus on 1-hop beacon dissemination, we get involved in the MAC layer broadcasting, which is quite different from the network layer broadcasting.*

As we know, a network protocol stack is structured in a layered architecture in which each layer offers services to the upper layer. The application layer is the upmost layer in the protocol stack and offers services to the user. To ease explanation, we define a virtual layer, called communication layer, as the combination of all layers under the application layer. This virtual layer normally, as the Open Systems Interconnection (OSI) reference model suggests, includes physical layer, MAC layer, networking layer, and transport layer. However, VANETs may be deployed with a rather different protocol stack and some layers may be absent [15]. For example, normally in beacon dissemination applications, only MAC and physical layers are present. Nevertheless, in the sequel of this section we continue with the general term “communication layer” to deal with more general cases.

Figure 13.2 shows three-layer architecture we consider in this chapter. The communication layer offers services (i.e., sending and receiving data) to the safety applications in the application layer, and, the safety applications are in charge of giving different life safety services to the passengers. In general, in networking literature there are two kinds of relationships between the QoS offered by the communication layer to the application layer and the one that the application layer offers to the users (in our context ‘passengers’).

1. In reliable data transfer protocols such as HTTP and FTP, the communication layer must guarantee reliability in terms of the delivery rate, even though it may lead to a large delay. Indeed, the role of the transport layer (such as TCP) is to compensate shortcomings of the lower layers, so that the application layer can offer satisfactory services to the user.
2. In real-time applications, normally it is not required that the communication layer offer fully reliable services to the application layer, because it may come at the expense of excessive delay, which is critical in those applications. In other words, the application layer tolerates some unreliability in the services offered by the communication layer.

* Beacon-based safety applications normally demand single-hop broadcasting at the MAC layer, while alarm-based safety applications and comfort applications usually demand multihop broadcasting/unicasting at the network layer.

While alarm-based safety applications and comfort applications may be kept in the first category, we believe that beacon-based safety applications can be categorized in the second group. Note that beacon messages do not contain unpredicted information (as the alarm messages do). Thus if the application layer does not receive fresh beacon messages from some vehicles for a short period, it can perform extrapolation to guess their status (e.g., speed, direction, position, and acceleration). It should be emphasized that extrapolation is not possible in the case of alarm messages, because alarm messages announce unpredicted events in which the new status of vehicles does not follow their previous status. Furthermore, when a fresh beacon message is received, the validity of the old one actually expires. Therefore, it is not needed that the communication layer struggle while retransmitting the old one. These considerations convinced us that beacon-based safety applications can get an advantage of some degree of tolerance in QoS offered by the communication layer. In other words, they function properly even though the communication layer is not able to offer a desirable QoS. Recent studies on DSRC show that single-hop beacon dissemination in VANETs is adequate in terms of delay, but the reliability remains defective [16,17]. Hence, in the following we concentrate on reliability as the main performance concern and consider beacon-based safety applications only.

For a given vehicle, we define a time window t by which the safety application must receive at least one fresh beacon from any neighboring vehicles. Let us denote by T the transmission interval of the communication protocol. Let p_{com} be the success rate of the communication protocol, which is the minimum among all delivery rates in a given transmission range of vehicles. Now the beacon-based safety application works adequately if at least one beacon among t/T beacons, from each neighboring vehicle, is received. In other words [16,17],

$$\begin{aligned} P_{\text{app}} &= 1 - P(\text{all failed in } N \text{ tries}) \\ &= 1 - (1 - p_{\text{com}})^{N} \\ &= 1 - (1 - p_{\text{com}})^{t/T} \end{aligned} \tag{13.2}$$

where P_{app} is the success rate of the safety application. It should be emphasized that the above equation is valid only if the message losses are independent, as we assume here. With Equation 13.2, one can simply relate the reliability of the application layer to that of the communication layer. In Figure 13.3, the relationship between reliability of the application layer and that of the communication layer is shown for different values of t (i.e., the time window as introduced above).

In order to design a safety application, the required attribute of the safety application should be extracted by traffic safety experts and then be used by the VANET protocol and application designers. So far in our model, each application is attributed by two parameters T and t. In addition, we define a vector α that represents the satisfaction levels for each QoS metric (e.g., delivery rate and delay). Table 13.1 shows our proposed attributes for each safety application.

Based on the above attributes, we can consider different classes of safety applications. For instance,

- Driver-assistant safety applications, which are expected to assist the driver in different maneuvers, such as lane changing and turning left/right. This class of applications can prevent various incidents that may happen because of the driver's fault. One example may be $95\% < \alpha < 99\%$ and $N \leq 3$. Note that the sufficient values for α and N should be determined by safety experts.

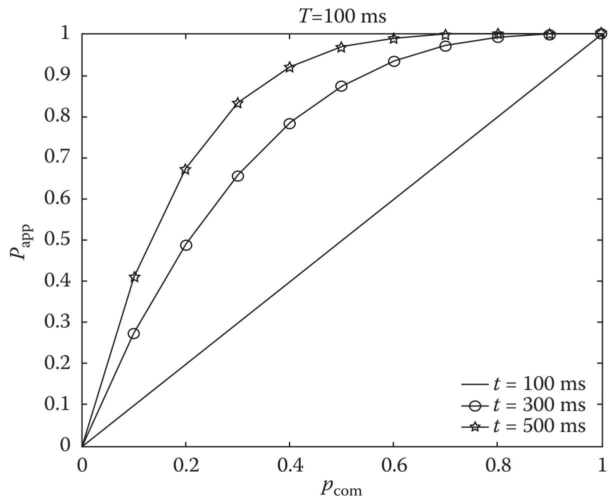


Figure 13.3 The relationship between reliability of the application layer and that of the communication layer.

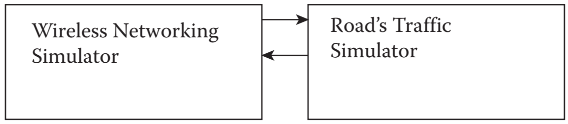
Table 13.1 Attributes of Beacon-Based Safety Applications

Attributes	*Description*
T	The time window in which the beacon-based safety application should receive at least one fresh beacon
T	The transmission interval of the beacon communication protocol
α	A vector comprising of satisfaction levels for QoS metrics of interest (e.g., delay and delivery rate)

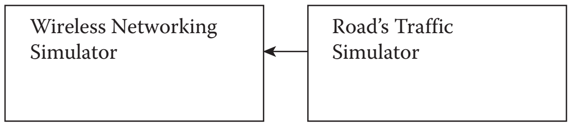
- Automatic safety applications, which are expected to control the vehicle as stand-alone systems. Undoubtedly, this class of applications requires restricted QoS satisfaction level. For instance, $\alpha > 99\%$ and $N = 1$. Note that the sufficient values for α and N should be determined by safety experts.

13.5 Simulation of Vehicular Networks

Although there are some efforts made by major car manufactures and research consortiums to establish prototype projects, simulation is still the most tractable and feasible way to evaluate new ideas in large-scale VANETs. Similar to other types of MANETs, there are well-known network simulators that may be invoked to conduct evaluation by simulation (more detailed explanation is provided later). However, it should be stressed that the main difference between VANETs and other types of MANETs is twofold: First, vehicle movement on roads follows sophisticated mobility patterns that are not modeled by means of random mobility patterns as used commonly in many other types of MANETs [18]. Moreover, there is a very mature knowledge on vehicle's mobility due to decades of research in transportation engineering as a field of civil engineering. Therefore, one aiming at simulation of VANETs needs to be familiar with fundamentals of traffic theory or



(a) Integrated co-simulation scenario for VANETs



(b) Integrated off-line simulation scenario for VANETs

Figure 13.4 Simulation scenarios in VANETs.

at least be able to make use of plenty of well-known traffic movement pattern generators (see some instances later in this section). Second, in many VANET scenarios the communication between vehicles may affect vehicle's mobility and vice versa. For example, a driver who is informed of a congested junction (through an alarm message) may decide to change his or her path and use an alternative path; thus, delivery of the message causes the change of the vehicle's movement pattern. On the contrary, the change of the vehicle's movement pattern affects road density and message dissemination. This means that we should be able to couple a network simulator to a road's traffic simulator. What is needed in this case is a co-simulation of the wireless network behavior and traffic's movement by which the aforementioned mutual interaction is actualized. However, many current research in VANETs is done by integrated off-line simulation, in which one-sided interaction is held (i.e., the wireless network simulator is fed by mobility patterns generated by the road's traffic simulator). Figure 13.4 shows a block view of the two possible simulation scenarios in VANETs.

13.5.1 Road's Traffic Simulators

Generally, traffic's flow can be viewed in either macroscopic or microscopic perspectives. In the macroscopic view, vehicular traffic is considered as fluid compressible medium. Thus, the basic rules of fluid mechanics are applicable. In particular, there is a basic equation that relates macroscopic metrics such as flow, density, and speed (see Equation 13.1). The macroscopic modeling of vehicular traffic is able to provide only general information such as road's capacity and density and does not consider individual vehicle's movement. On the contrary, the microscopic perspective of vehicle's traffic takes into account each vehicle's movement. Thus, many sophisticated aspects of vehicular traffic such as car-following models (i.e., mutual interaction between vehicles while traveling along roads) can be modeled. As a result, microscopic traffic simulators are more suitable for VANETs research.

There are many proprietary road's traffic simulators such as Paramics [19] and CORSIM [20] that are able to model vehicular traffic in great detail, but without loss of generality, here we focus on free or open source simulators that can be used easily for public research. Nowadays, many of such simulators are presented. At the time of this writing, the most important vehicle's mobility generators include SUMO (simulation of urban mobility) [21], MOVE (mobility model generator for vehicular networks) [22], FreeSim [23], City Mov v.2 [24], VanetMobiSim [25], and STRAW (street random waypoint) [26]. Decision on choosing a particular software should be taken based on the requirements of the simulation scenario in hand. A detailed explanation on a particular simulator is beyond the scope of this book. However, a clarifying and good comparison between these simulators and some others is provided in [27].

13.5.2 Wireless Network Simulators

In this case, all simulators that are usable in other types of MANETs can be of use. The most important proprietary simulators include OPNET [28] and QualNet [29]. However, the most important and commonly used free or open source software are the following: Network Simulator 2 (NS-2) [30], Global Mobile system Simulator (GloMoSim) [31], Objective Modular Network Testbed in C++ (OMNET++) [32], Java in Simulation Time/Scalable Wireless Ad hoc Network Simulator (JiSt/SWANS) [33], SNS (a staged network simulator) [34], and NCTUns (National Chiao Tung University Network Simulator) [35]. It should be noted that GloMoSim is no longer supported and a new version of it is present under the title of the proprietary software QualNet.

13.5.3 Integrated Off-Line Simulation of VANETs

It should be noted that almost all traffic simulators are able to generate mobility patterns for famous wireless network simulators, including NS-2, OMNET++, and GloMoSim (QualNet). Such information can be easily accessible from manual documents of the above-mentioned traffic simulators. Therefore, conducting integrated off-line simulations is a straightforward task. Indeed, most of the simulations in the current literature can be classified in the category of off-line simulations. In other words, a wireless simulator is fed by a mobility pattern generated by a road's traffic simulator. Although in many cases this issue suffices, for many other cases one may need online simulation (co-simulation) to be able to take into account mutual interactions between a traffic simulator and a wireless network simulator.

13.5.4 Integrated Co-simulation of VANETs

Currently, quite a few of these simulators are available and their usage is not that much common in the research community. As mentioned above, due to the special characteristics of VANETs there should be an integrated simulation framework by which both road's traffic and the wireless network aspects of the problem are simulated. Most of the software (except NCTUns) are indeed third-party projects that are developed on top of two other simulators: a road's traffic simulator and a wireless network simulator. In the following, we list the most important ones available at the time of this writing:

a. TraNS (traffic and network simulation environment) [35]: It is written in C++ and Java and facilitates co-simulation between NS-2 and SUMO. It was developed and supported by EPFL, Switzerland.
b. Veins (vehicles in network simulation) [36]: TraCI (traffic control interface) modules for co-simulation of SUMO with OMNeT++ and JiST/SWANS. TraCI is a client/server architecture for connecting to SUMO, in which SUMO behaves like a server that interacts with a client. It was developed by Christoph Sommer et al. in University of Erlangen, Germany.
c. NCTUns [37]: In contrast to the above two software, it has built-in capability to support integrated co-simulation of vehicular traffic and wireless network. NCTUns is a powerful and general-purpose network simulator that has been extended to VANET simulation. The mobility patterns generated by NCTUns are claimed to show a good agreement with those of common traffic simulators.

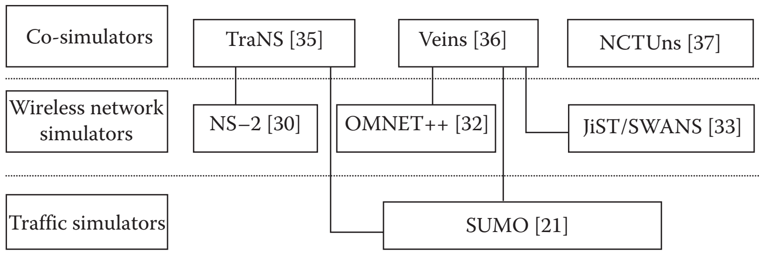


Figure 13.5 Taxonomy of tools for integrated co-simulation of VANETs.

Figure 13.5 shows the most important tools available to conduct integrated co-simulation of VANETs. Note that the case of integrated off-line simulation is not shown here due to plenty of alternatives.

13.6 Transport Layer Protocol for VANETs

VANETs are supposed to be connected to other wireless as well as various wired networks. Therefore, to offer a standard application interface (e.g., socket-like interfaces), one may consider standard protocols such as TCP (transport control protocol) and UDP (user datagram protocol) (and their enhancements) as transport layer protocols of VANETs. TCP is a well-known connection-oriented and reliable protocol operating in the transport layer of the OSI model. This protocol is relied on Acknowledgment (ACK) to be sure about the delivery of each segment of data; thus, it is normally resorted for applications in which reliability is critical. TCP treats data as an ordered sequence of packets and uses retransmissions to guarantee that from the receiver's point of view, all packets are received in order. As a result, a reliable and in-order reception of each piece of data is promised. While UDP is a connectionless and unreliable protocol in which neither reliability nor in-order reception of data is supported. Indeed, the most important feature of UDP is to provide a socket-like interface to the application layer (through defining port numbers in its header). Choosing a particular protocol directly depends on the QoS requirement of the application in hand. In the following we discuss this issue.

13.6.1 Transport Layer Protocol for Safety Application

From Section 13.4 we know that safety applications are characterized by tough timing requirements. In many safety applications, late reception of a message is as bad as nonreception of it. Therefore, it is easy to deduct that TCP does not suit safety applications due to the following reasons: (1) Connection establishment (i.e., three-way handshaking mechanism) is time-consuming, which might jeopardize timing requirement of safety applications. (2) TCP uses a closed-loop reliability mechanism (based on ACK) and tries to retransmit lost packets until they are received successfully. However, for many safety applications it might be better to send a fresh message (conditioned on that the message is repeatable) instead of insisting on resending the previously issued one.

Generally speaking, using TCP for safety applications in VANETs is not justified and instead UDP is more suitable. However, for some cases when the safety message is not repeatable, the effort of the application layer is beneficial for compensating the poor reliability of UDP. One example of unrepeatable safety messages may be an alarm message announcing an icy surface. If the vehicle receiving this message is disconnected from other approaching vehicles (due to intermittent connectivity of VANETs), then it should keep the message (in the application layer) or deliver it to an RSU (roadside unit), with the aim of not losing the alarm.

13.6.2 TCP for Comfort Applications in VANETs

On the one hand, many comfort applications are based on bulk data exchange (e.g., file download) or long-lasting data connections (e.g., HTTP). These applications require in-order and reliable exchange of packets. On the other hand, we know that VANETs suffer from intermittent connections due to movement of vehicles [38]; thus, the amount of packets that may be received successfully varies with the traffic pattern, and the order of received packets may not be preserved. Furthermore, an exchange of ACK packets in such intermittently connected network results in increasing traffic load of the network and thus leads to increase of interference and collision level in the MAC layer of the DSRC standard (which is based on IEEE 802.11p). Since IEEE 802.11p is based on the CSMA/CA mechanism, the aforementioned collisions are too restrictive and thus cause poor throughput of TCP connections.

TCP is originally proposed for wired Internet; thus, it suffers from many shortcomings when used for wireless networks. The main problem is that TCP is not able to distinguish between error-prone links and network congestions, which leads to unnecessary slow-start mechanisms. Generally, the previous works tried to modify the congestion control of the TCP (e.g., freeze-TCP [39]) or to use information of intermediate nodes such as Explicit Congestion Notification (ECN) (RFC 3168). There are many works that use TCP for MANETs, which are reviewed in [40] in great detail. Moreover, there are a few works that address TCP challenges for VANETs in particular [41]. However, it seems that TCP has an inherent weakness for such intermittently connected topology as VANETs. Therefore, one may use other approaches for tackling this problem. In the following section we present an example of such methods.

13.6.2.1 Use of UDP Along with Forward Error Correction Techniques

The troublemaking point of TCP in VANETs is its congestion control mechanism through which it reacts whenever the network is disconnected temporarily. If one uses UDP (instead of TCP), the problem related to congestion control is solved, but it is still needed to compensate for the lack of reliability of the UDP. One solution for this problem is to make use of UDP (instead of TCP) along with an application layer protocol based on FEC (forward error correction) to satisfy reliability. In fact this method is based on an open-loop reliability mechanism in which there is no need for any ACK of data packets and retransmission of packets. Instead, probable errors are corrected by taking advantage of some redundant data that have been sent along with the original data.

In a proposed algorithm [42], Yousefi et al. made use of fountain coding as an FEC approach for a category of applications in VANETs that are based on file downloading. The term *fountain* refers to the fact that the only thing that the receiver needs to be able to reconstruct the original input symbols (packets) is to receive a minimum number of *any* output symbols (packets). Let k be the original number of packets that constitute the file to be transmitted, and let n be the total number of packets that need to be received at the receiver so that it can decode the original content. We have $n = k(1 + \varepsilon)$, where ε, termed the decoding efficiency, ranges typically between 10 and 100% (normally in the range of 5–10%), depending on the specific implementation [43]. Please note that when the receiver receives the n symbols, decoding is successful with a probability equal to $(1 - \delta)$, where δ is upper-bounded by $2^{(-k\varepsilon)}$. This means that larger file sizes and/or higher values of ε make the decoding probability even larger. As of complexity, it may be as low as linear in the number of coded symbols.

Among the potential applications of VANETs (safety and comfort applications), we believe that using fountain coding best suits comfort applications. This is because in safety applications we normally encounter a small number of bytes (in the scale of a few kilobytes) to be transmitted and thus there is no need to chop a safety message into pieces. Furthermore, due to restrict delay requirements of the safety message, the time overhead of coding and decoding algorithms might be intolerable by the majority of safety applications.

In the proposed approach of [42], the sender vehicle encodes files using a sample of fountain such as Raptor [44] (or the files may be encoded off-line and stored in the memory of the sender). Then the sender sends a train of encoded packets toward the receiver using the UDP protocol in the transport layer, such as a fountain that spreads water drops. In the beginning of a file transmission, the sender declares the amount of packets of the original file, size of each packet, and the coding algorithm. When the packets arrive, the receiver tries to decode the file using the same coding algorithm. Whenever the amount of received packet is enough, the receiver sends a message to the sender and asks to stop sending packets. Note that the sufficient amount of packets for successful encoding is just slightly larger than the amount of actual file packets. But there is no need to receive packets in a special order and all packets have an equivalent value for the receiver vehicle.

Figure 13.6 shows the number of completely downloaded files of the above-mentioned technique named as fountain as well as the ordinary FTP (which make use of TCP). This metric is important for comfort applications because due to their nature, vehicles can make use of such an application only if the related file is downloaded completely. In the conducted simulation, 30 vehicle pairs are chosen such that their hop count distance is less than 4 (at the initiation of the communication).

As shown in Figure 13.6, the fountain scenario outperforms the FTP scenario. However, as one can conclude from the figure, in most of the cases we observe a poor performance in terms of number of completely downloaded files. Since this is inevitable due to the dynamic nature of the traffic, we need to provide a resume facility. In other words, vehicles could be able to continue their incomplete download from other vehicles somewhere else and/or some time later. The use of fountain coding can best fit this requirement because each neighboring vehicle may have different packets from a file. In such a situation, a given vehicle can reconstruct the file whenever it is able to collect enough distinctive packets from neighboring vehicles. Obviously, this demands some

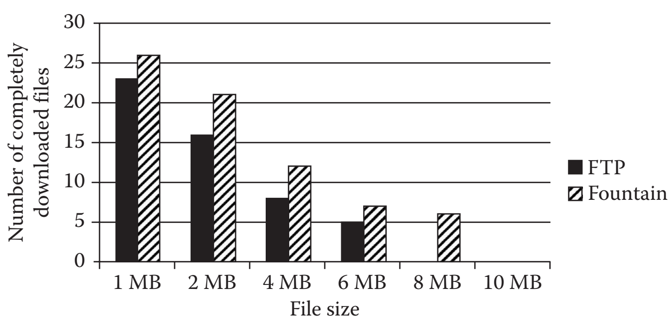


Figure 13.6 Comparison of fountain and FTP scenarios: number of completely downloaded files (out of 30). (From Yousefi, S., Chahed, T., Moosavi, M., and Zayer, K., Comfort applications in vehicular ad hoc networks based on fountain coding, In IEEE WiVec 2010, Taipei, May 2010. © (2010) IEEE. With permission.)

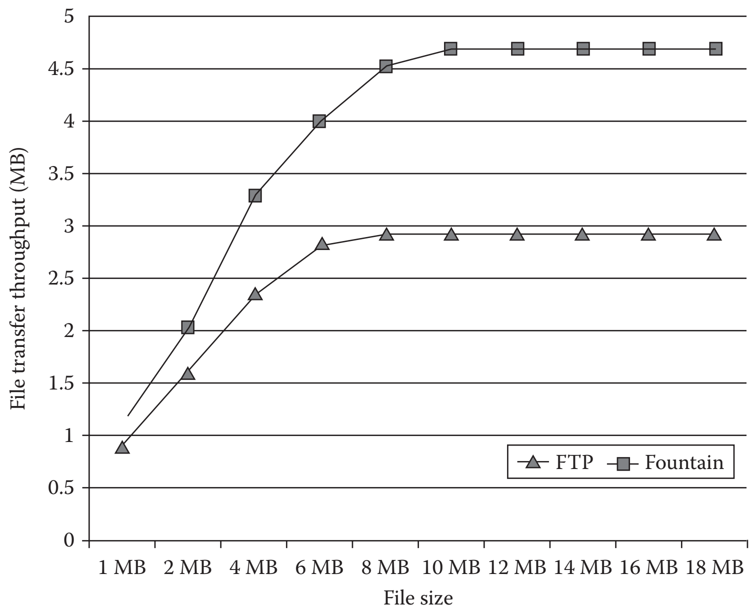


Figure 13.7 Comparison of fountain and FTP scenarios: average byte throughput. (From Yousefi, S., Chahed, T., Moosavi, M., and Zayer, K., Comfort applications in vehicular ad hoc networks based on fountain coding, In IEEE WiVec 2010, Taipei, May 2010. © (2010) IEEE. With permission.)

support from the application layer. On the contrary, in the case of FTP, the vehicle would need to collect specific packets (based on the predefined order) that may be hard to obtain from neighboring vehicles. In order to evaluate this capability of fountain, Figure 13.7 shows byte throughput of the fountain and FTP algorithms. This metric is important since vehicles may be able to resume the download some time later or from some other vehicles. As followed from the figure, the fountain scenario's throughput in terms of byte count is higher than the FTP scenario's. Indeed, by taking advantage of fountain coding we can transfer larger files in comparison to the case when a classic FTP algorithm is used. It is mainly because fountain scenario neither uses retransmission mechanism nor needs in-order packet delivery. In other words, in fountain all file chops have equivalent value, and if one is lost, it can be replaced by another one easily.

13.7 Vehicle to RSU Communications

As mentioned before, vehicular networks exist in two different architectures: V2V and V2I. In the V2V case, which is essential for safety applications, a pure ad hoc network between moving vehicles is established, whereas in the V2I case, vehicles and roadside infrastructure construct a hybrid ad hoc network. The latter is suitable mostly for comfort applications, even though there are also some safety applications that rely on V2I architecture. It is expected that data access from RSUs will become crucial in the near future [45]. Currently, it is assumed that RSUs are equipped with DSRC technology and thus use the IEEE 802.11p MAC layer. However, due to advances in mobile WiMAX (worldwide interoperability for microwave access), it is quite predictable that WiMAX technology is applied in this case (see some more discussion in Section 13.12). Among different applications of VANETs, comfort applications are more significant candidate for vehicle to RSU communications. It is mainly because the delay incurred for transmission from a vehicle to RSU and from the RSU to another vehicle may violate timing requirement of many safety applications. Of course, for some alarm-based safety applications in which an unrepeatable alarm is generated, RSUs can be used to buffer the alarm until an interested vehicle arrives.

Commonly, RSUs can act as a buffer point between vehicles or act as a router for vehicles to access the Internet. Besides, the RSUs may act as servers and thus provide various types of information to vehicles on roads. The following instances are some examples for RSU applications:

1. WEB applications: The passengers can connect to the Internet and make use of various applications such as checking e-mails and browsing Web pages or other Web applications.
2. Real-time traffic: Vehicles can report real-time traffic observations to RSUs. The traffic data then can be transmitted to a traffic center. The result of traffic data analysis then can be accessible to vehicles moving across each RSU.
3. Digital map downloading: When vehicles are driving to a new area, they may hope to update map data locally for travel guidance, such as changing unilateral or deadlock roads.
4. Commercial advertisements: When a vehicle arrives at a new area, it is very helpful to receive local advertisements on hotel reservation, parking places, latest price of petrol, and other stuff. In this case, video and audio advertising files are to be broadcasted by different companies.

In the following we consider an urban environment in which an RSU is established in each junction. Technical challenges in this case can be categorized into intra-RSU and inter-RSU challenges.

13.7.1 Intra-RSU Scheduling

As shown in Figure 13.8, the RSU established in a junction is in charge of serving vehicles that are moving through the cross-road. Actually the RSU responds to the requests submitted by the vehicles. On the one hand, each vehicle stay in the RSU area for a short period of time, and on the other hand, by increasing the number of vehicles (and thus requests), the bandwidth limitation becomes an important challenge. Therefore, it is important to use a scheduling policy to maximize the number of served requests. Besides, some requests that have higher priority should be taken higher priority of service.

In [46], Zhang et al. proposed a scheduling algorithm that is summarized in the following. Each vehicle's request is characterized by a 4-tuple: <*v_id, d_id*, *op, deadline*>, where *v_id* is the identifier of the vehicle, *d_id* is the identifier of the requested data item, *op* is indicating the operation (upload or download), and *deadline* is the time constraint of the request. If a request is not served within the deadline time limit, it will be dropped from the waiting queue (e.g., the service queues in Figure 13.8) of RSU since the related vehicle is no longer under RSU's coverage. Having this information, the RSU uses scheduling policy to maximize the number of served requests. For this purpose, a scheduling algorithm called D*S has been proposed in which both data size and request deadline are considered. For more detailed discussion and results, please refer to [46].

An open problem and challenge here is to consider multiclass requests. Indeed, in [46] two classes have been mentioned: upload and download. As shown in Figure 13.8, one can consider more sophisticated case in which different QoS classes such as video, audio, and data (text) are distinguished. Therefore, studying different queuing policies such as WFQ and WRR can be taken into account in both simulation and analytical points of view. Furthermore, since many vehicles may have the same requests, invoking multicast approach leads to a higher performance

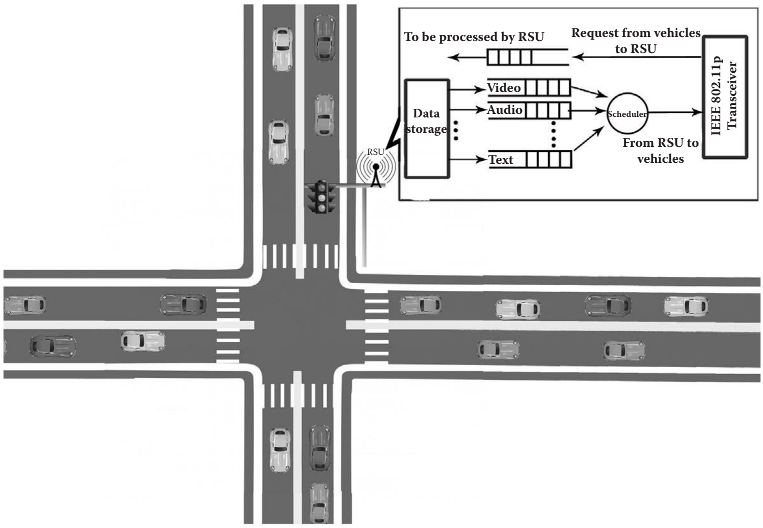


Figure 13.8 Intra-RSU scheduling scenario.

in terms of the number of served requests. In this case the scheduling algorithm should maintain a trade-off between the number of multicast requests and unicast requests which are given service.

13.7.2 Inter-RSU Scenario

If we extend the previous case to an urban environment, an anticipated scenario would be one in which several RSUs are installed in each cross-road. Thus, vehicles moving out from a RSU's range will move into another RSU's range after some time. In other words, the service that is stopped in the first RSU can be resumed in the next RSU. This issue necessitates scheduling algorithm through which RSUs cooperate in order to maximize the number of served requests. Furthermore, reducing delay for individual requests would be another goal of scheduling algorithm. Since the number of vehicles and RSUs as well as the number and size of files are potentially large, scalable scheduling is a challenge. It should be recalled that as a realistic assumption we consider that the RSUs are connected by another network (a wired network or a wireless one such as WiMAX) and managed by a service provider or a group of joint service providers.

In [47], Shahverdy et al. studied a sample of aforementioned problem of file downloading. It is assumed that the files are uploaded by the service provider through the network of RSUs. Therefore, the scenario suits comfort applications only. A vehicle may not be able to finish its download from an RSU; thus, the proposed algorithm allows it to continue its download from the next RSU. In the proposed scheduling algorithm, each RSU implements two separate queues for (1) download requests from the scratch and (2) download requests that are resumed. The data for distribution are chosen from aforementioned queues based on some scheduling policies. A scenario of the problem is depicted in Figure 13.9.

Vehicles retrieve their data from the RSU when they are in the RSU's coverage range. The RSU (server) maintains a service cycle, which is non-preemptive; i.e., one service cannot be interrupted until it is finished. All vehicles can send request to the RSU if they tend to access the data. Each request is characterized by a 5-tuple: <*v-id*, *d-id*, *w-RSU*, *s-rec*, *deadline*>, where *v-id* is the

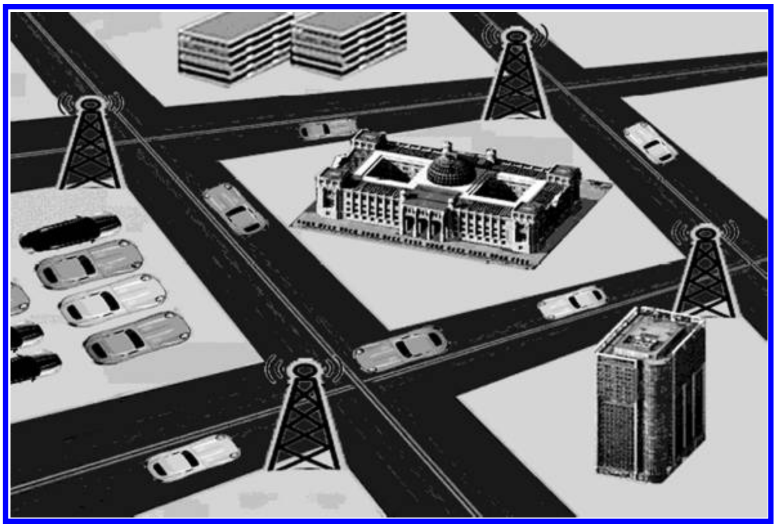


Figure 13.9 A scenario with multiple RSUs that demands inter-RSU scheduling.

identifier of the vehicle, *d-id* is the identifier of the requested data item, *w-RSU* identifies the RSU from which the vehicle has come, *s-rec* is the identifier of the data size that is received until now from the previous RSU (the vehicle now asks for downloading the remaining data from the current RSU), and *deadline* is the critical time constraint of the request, beyond which the vehicle moves out from the RSU area. Each vehicle is equipped with a GPS (global position system); therefore, vehicles know their own geographical position and driving velocity. Therefore, a vehicle can estimate its leaving time, which indeed is the service *deadline*, mentioned above. The scheduling policy adapted here is D*S, which is originally proposed in [46].

Open research problems in this case can be the following. Similar to the case of intra-RSU, one can extend the model to different QoS classes (video, audio, ordinary data). The trade-off between multicast and unicast requests is also challenging in particular because of multiple RSU architecture. Another important issue that is very critical in realizing the idea in real life is to consider the following problem. Take m files (containing l chops) and n RSUs and T be the average request deadline (the average time a vehicle is in the coverage area of an RSU). Then one may face a distributed file download case, which can be solved as a maximization problem. The details of such a problem and objectives are needed to be investigated, but maximizing number of served requests and minimizing average download delay can be considered as objective functions.

13.8 Beacon-Based Safety Applications

As mentioned in Section 13.4.1, single-hop beacon dissemination is sufficient for most of the safety applications. However, there is an ongoing debate on whether multihop beacon dissemination would be necessary. Recent results show that multihop dissemination of beacons (periodic safety messages) results in high imposed load on the wireless channel and poor performance of DSRC systems. The main reason here is that DSRC is using IEEE 802.11p, an alternative of IEEE 802.11, which is based on the CSMA/CA paradigm. For a good discussion on this issue, an interested reader may refer to [48]. The following discussion is mainly focused on single-hop message

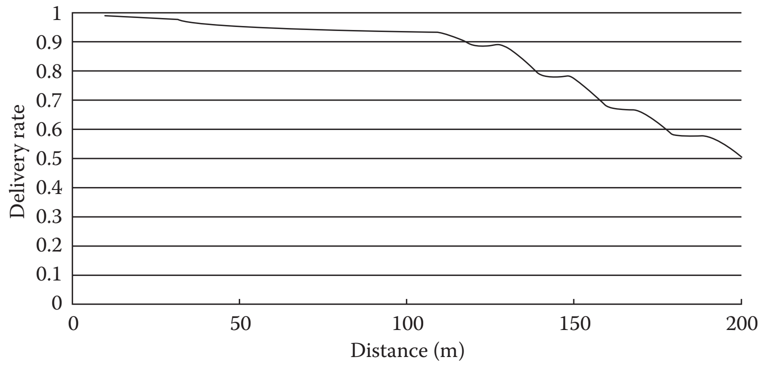


Figure 13.10 Delivery rate of beacons in terms of distance from the sender.

dissemination; however, since multihop dissemination is based on single-hop dissemination, the results may be usable there.

To show the effect of the distance on beacon reception rate, in Figure 13.10, we show the result of a simple beacon dissemination protocol [49] where the vehicles' transmission range is 200 m. The transmission interval is 200 ms and the packet size is 500 bytes. As followed from the figure, the delivery rates are decreasing dramatically by increasing the distance from the sender. This indeed means poorer safety coverage by the beacon-based safety application. We can describe this border effect mainly by a well-known hidden terminal problem. A hidden terminal is one that is within the range of the intended destination but out of the range of the sender. The partial solution to this problem is the use of RTS (ready-to-send)/CTS (clear-to-send) packets. RTS/CTS signaling may solve the problem for unicast communication, but in IEEE 802.11 the RTS/CTS mechanism is not invoked in the broadcast scenarios mainly because CTS messages sent by multiple receivers will result in severe collisions. Hence, the hidden terminal is more troublesome in the broadcast mode of the IEEE 802.11 MAC layer.

Observing such a low delivery rate, the important question that would arise is how to alleviate such an adversity in order to get acceptable QoS for safety applications. The main approach is to control the wireless channel's load. The following factors are the most important ones that should be controlled in order to reduce channel's load:

- Transmission range: While higher transmission range results in larger awareness distance and is better from the safety point of view, it leads to a larger interference domain. As a result, packets are more likely to collide with each other and throughput degrades more severely. A good example of approaches that are based on controlling power (transmission range) for alleviating channel's load is that of [50].
- Transmission interval: This parameter is directly related to the requirements of the safety applications and should be determined based on vehicle's speed and driver reaction time, and traffic density. While a smaller transmission interval can prevent unsafe situation in higher speeds and more unsafe conditions, it results in more saturated channels and so it is more likely to cause collision between simultaneous transmissions. An example of works that consider increasing transmission interval (decreasing transmission frequency) is that of [51], which will be discussed briefly in the following subsections.
- Packet payload size: To estimate the packet size value, we consider that every packet will contain several parameters composing the state of the sender especially location, speed, road

hazards, etc. Also, there should be some aggregated information about sender's neighbors. In addition, by including security issues that are very important in intervehicle communication, we can reach packet sizes ranging from 100 to 500 bytes for each message. Generally, safety messages with the size of 1 Kbyte are not far from expectation. An example of works that consider an increase of packet payload size (and simultaneously decreasing transmission frequency) is that of [51], which will be discussed briefly in the following subsections.

- Control of dissemination pattern: In IEEE 802.11p when the MAC layer is given a packet to disseminate, it starts the process of dissemination (contention phase, etc.) immediately without any knowledge about other vehicle's status. This is inevitable due to MAC's properties. One promising approach is to control the pattern through which the MAC layer is given packets from upper layers (e.g., application layer). In other words, the application layer (i.e., the safety application) can take advantage of a scheduling algorithm using which packets are delivered to the vehicle's MAC layer in a specified order. Therefore, collisions can be avoided and the performance will be improved noticeably. An example of works that consider scheduling algorithm in the application layer is that of [52], which will be discussed briefly in the following subsections.

In the following, we mention two examples of proposed methods that address the problem of controlling wireless channel load, with the aim of decreasing collision level.

13.8.1 Estimation-Based Beacon Dissemination

Although more accurate information (i.e., a larger packet size) could provide safer situation, as argued in the previous subsection, increasing packet size may lead to more saturated channels and as a result more collisions. Nevertheless, due to the nature of CSMA/CA, it could be intuitively understood that the effect of increasing packet size on the performance is not as adverse as the effect of reducing transmission interval. The reason is that acquiring the channel for several transmissions is the bottleneck of CSMA/AC-based MAC protocols. Therefore, one promising idea can be increasing packet size instead of increasing transmission interval (decreasing transmission frequency). To substantiate the idea without hindering the safety level, one possible approach is to estimate several next beacons by using some estimation techniques and send them in advance. In [51,53] a method is proposed that uses the Kalman filter estimation. In the following, we briefly explain the approach suggested in [51].

It is assumed that each vehicle periodically obtains its location, speed, acceleration, etc., through a GPS and/or in-vehicle sensors at every time step. Then the Kalman filter algorithm is implemented in the vehicle to estimate the future longitudinal and lateral location of the vehicle. The Kalman filter [54] is a set of recursive mathematical equations that provide an efficient recursive computational means to estimate the state of a process (here the intention is to estimate future longitudinal and lateral location of the vehicles) in a way that it minimizes the mean of the squared error. As illustrated in the block diagram of Figure 13.11, only one estimator is implemented in each vehicle. The Kalman filter block is in charge of estimating next location information for several future time steps in advance.

Every beacon message contains two categories of information: measured values for the current time step and estimated values for several future time steps. The rationale behind our approach is to prevent dissemination of unnecessary information. The scheduler block in Figure 13.11 is responsible for such a decision: whether any further transmission is necessary or not. In each time step, the location information reported by the GPS is compared with the estimated locations for

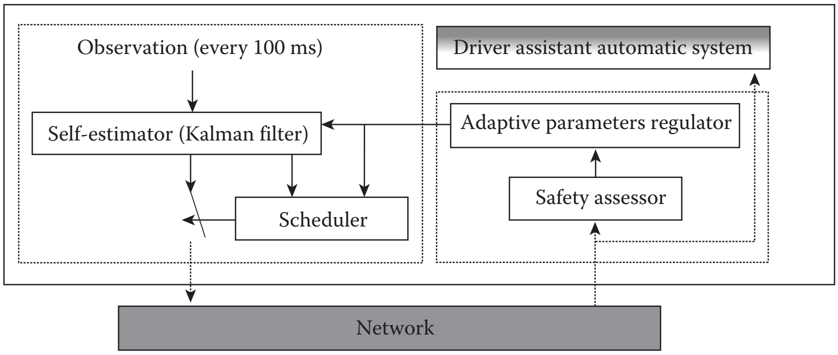


Figure 13.11 Block diagram of the proposed method. (From Armaghan, M., Fathy, M., and Yousefi, S., *FGCN 2009, Korea. Communications in Computer and Information Science* (CCIS Book Series), Berlin: Springer, vol. 56, pp. 74–82, 2009. With permission.)

the same time step (which has been transmitted ahead). When the estimations' error is below a threshold, there is no need of fresh transmissions. Otherwise a new beacon message is composed, containing both present information and estimated information. However, fresh transmission is also done if no estimations are available for a specific time step.

There are two important parameters of the algorithm that play a critical role in the safety level offered by the proposed approach: the threshold of lateral and longitudinal location estimation error and the number of estimated steps. The former is considered as a criterion for initiating fresh beacon transmission as explained above. The latter is indeed the number of time steps for which the estimated data transmitted have been calculated and transmitted ahead. As this number is increased, the consecutive time steps during which no fresh transmissions are performed increased, which causes less crowded wireless medium. However, it should be stressed that there is a trade-off between the safety level and the number of fresh transmissions. On the one hand, disseminating fresh measured information at every time step is obviously very desirable from the safety point of view, but this may lead to increase of the collision level and thus frequent losses take place. On the other hand, relying on estimated data for a large number of time steps may lead to deterioration of the safety level due to limited capability of the estimator as well as the possibility of sending very large packets. Therefore, the value of aforementioned parameters should be determined intelligently. The detailed parameter setting for Kalman estimation as well as other parts of the approach can be a subject of further research but some outlines are provided in [51]. However after being set, the above parameters are saved in the adaptive parameter regulator block, depicted in Figure 13.11.

In Figure 13.11, there is another block (safety assessor) that is in charge of safety assessment through determining whether the current setting of parameters provides enough safety for the vehicle. This block is a critical block and should be implemented based on the knowledge of safety experts and one may use artificial intelligent (AI) decision-making algorithms. Actually, the output of this block is used for setting the values of necessary parameters in the adaptive parameter regulator block.

Design of any block of Figure 13.11 is an open research problem, which is indeed very critical for the success of the safety application. In particular, the use of various estimation techniques can be investigated to reach the better estimation accuracy. Besides, the role of the safety assessor in determining whether a state is safe is a serious challenging problem. In fact, until now there is no clear definition of safe state in the literature of VANETs. Due to the indefinite nature of safety, it seems that one should resort to AI techniques in order to define the level of safety for a given state.

13.8.2 Application Layer Scheduling

As mentioned throughout this chapter, one of the most important challenges with DSRC-enabled services pertains to its IEEE 802.11p MAC layer, which is at risk of extensive collisions in saturated channels. Although these collisions are inevitable due to the nature of the MAC layer, one may think of other alleviating approaches to decrease such collisions. The results could certainly lead to higher beaconing rate and effective range. To fulfill this goal, one possible idea is to do scheduling in the application layer. In other words, vehicles cooperate with each other to disseminate their beacons in a specific order; thus, collisions are removed ideally. In the following, we explain an approach proposed in [52], pursuing the aforementioned idea adapted from the idea of space division multiple access (SDMA) applied in [55].

In the proposed approach, the road is divided into a series of sections (clusters) in which only nonadjacent sections transmit the beacon message simultaneously. Each section is further subdivided into several subsections where only one vehicle can be placed in each subsection. What causes this method to be efficient is the fact that only one subsection (i.e., the vehicle positioned there) can transmit once. Figure 13.12 shows the overall architecture of the proposed method. As followed from the figure, the method is based on a clustering mechanism where all odd-number clusters (e.g., CS1, CS3, and CS5) transmit simultaneously. After a delay that should be computed, the even-number clusters (e.g., CS2, CS4, and CS6) start transmitting at the same time.

During the cluster formation step, a series of contiguous clusters are arranged along the road so that any cluster has a unique cluster-head vehicle (CV). After the end of the cluster formation, each CV broadcasts a Hello message (HM) to announce its current position to the other vehicles in its corresponding CS. Then in order to transmit beacons free of collisions, a kind of SDMA mechanism is employed. To reach this goal, each CS is subdivided into N segments as follows:

$$N = \frac{2R}{L_s} \tag{13.3}$$

where R is the transmission range of the CV and L_s is the minimum allowed distance of two vehicles. Recall that $2R$ is the length of each CS. If the road has M lane, there are B road blocks in each CS as follows:

$$B = M \times N \tag{13.4}$$

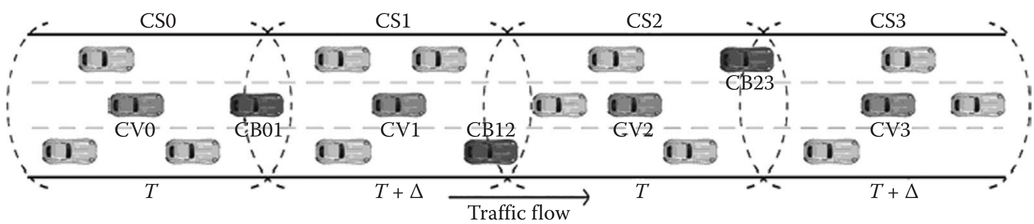


Figure 13.12 Cluster synchronization. (From Sadatpour, V., Fathy, M., Yousefi, S., Rahmani, A.M., Cho, E.-S., and Choi, M.-K., *FGCN 2009, Korea. Communications in Computer and Information Science* (CCIS Book Series), Berlin: Springer, vol. 56, pp. 133–140, 2009. With permission.)

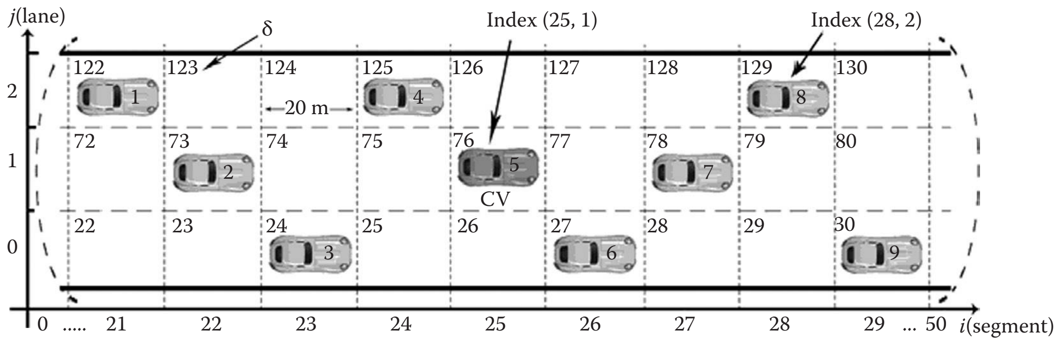


Figure 13.13 Road block partitions and time-slot label assignment for $M = 3$ and $N = 50$. (From Sadatpour, V., Fathy, M., Yousefi, S., Rahmani, A.M., Cho, E.-S., and Choi, M.-K., *FGCN 2009, Korea. Communications in Computer and Information Science* (CCIS Book Series), Berlin: Springer, vol. 56, pp. 133–140, 2009. With permission.)

where only one vehicle can be located in each block. Each road block is identified with index (i, j), where $0 \le i \le N - 1$ and $0 \le j \le M - 1$. As shown in Figure 13.13, each road block is assigned a time-slot label as

$$\delta = i + j \times N + 1 \tag{13.5}$$

Then each vehicle sends its beacon message in accordance with its own road block; thus, each vehicle should be able to identify its own block. For this purpose, it should be able to determine the index (i, j). It is assumed that each vehicle is equipped with digital maps and it can use its own GPS receiver to recognize its lane; thus, j can be identified for any vehicle. Furthermore, each vehicle can determine i (segment) using the following formula:

$$i = \left\lfloor \frac{R}{L_s} \right\rfloor + \left\lfloor \frac{X_v - X_{cv}}{L_s} \right\rfloor \tag{13.6}$$

where X_v and X_{cv} are the x-coordinate of the vehicle and CV, respectively. For example, Figure 13.13 shows an example for obtaining values of δ for $R = 500$ m, $L_s = 20$ m. The vehicle number 9 can identify index (i, j) using its own GPS receiver and (13.6) (in the figure, $X_{cv} = 25 \times 20 = 500$ m and $X_v = 29 \times 20 = 580$ m). Note that each vehicle is aware of the x-coordinate of its cluster's CV (i.e., X_{cv}) through the HM send by each CV after cluster formation. Thus, it can obtain $\delta = 130$ by using (13.5) and send its message at the $130t + T_{Hello}$, where t is the transmission interval and T_{Hello} is the time when HM was issued. As shown in Figure 13.12, collisions may happen if vehicles belonging to adjacent CSs send beacon messages simultaneously. To avoid this problem, the even-numbered CVs will send HM at T_{Hello} and the odd-numbered CVs will send it at $T_{Hello} + \Delta$, where

$$\Delta = B \times t \tag{13.7}$$

There are several open problems regarding this topic. First, in the proposed approaches, slot allocation is performed based on fix geographical positions, no matter any vehicle exists in the related road block or not. Therefore, one enhancement for this approach is to consider adaptive slot allocation based on traffic's density. In other words, if a given cluster contains fewer vehicles, then the scheduling algorithm can assign more dissemination tickets to those vehicles. Another important problem here is cluster maintenance. This problem is serious due to dynamic topology of VANETs, in particular if the opposite direction traffic is included in the desired safety application. When vehicles leave their home cluster and enter another cluster, the slot allocation of both clusters should be changed. If vehicles disseminate based on the previous allocated slots (in their own home clusters), the disseminated beacons will collide with other dissemination vehicles in the adjacent cluster. The solution here is to initiate the cluster reformation (maintenance) process. One can try to suggest an approach based on which such increasing collisions are detected and, if necessary, reformation of cluster is triggered. In the current approaches, such maintenance is triggered with a fixed and predetermined period.

13.9 Connectivity in VANETs

Connectivity is the primordial condition for message exchange in any network including VANETs. In a mobile network, connectivity is mostly affected by the mobility pattern of nodes. That is, nodes are not able to communicate, since they are not in each other's transmission range. Even when two given nodes are in the transmission range of each other, they may not be able to communicate due to radio interference (e.g., shadowing and fading) and some protocol issues (e.g., collisions due to hidden terminal problem in CSMA-based MAC layers). Therefore, research on connectivity is mostly focused on two things: connectivity impairments due to nodes' mobility and connectivity impairments due to radio and protocol factors (including radio interference and channel's effect such as fading and shadowing and MAC layer problems). In this chapter we focus on the former case.

Although there are many works on the investigation of the effects of mobility on connectivity in other types of MANETs, the obtained results can be hardly applied to VANETs. The reason is that for many other types of MANETs, usually random mobility patterns are taken into account [18]. But vehicular mobility cannot be fallen in the category of common mobility models.

When traffic is in the forced-flow phase, vehicles are closed to each other, and due to a typical transmission range of DSRC (a few hundred meters) the established ad hoc network is always connected. However, here the effect of interference may hinder connectivity. One way to tackle such a problem is to control power by which one can decrease the collision domain of nodes [50,56,57]. However, in such an attempt, safety requirements should be taken into account, according to which the vehicle's transmission range should not be fallen below a threshold (refer to Section 13.4.1). In the free-flow traffic phase, however, vehicles are moving freely due to their distance from each other. Thus, connectivity is affected by road's traffic characteristics as well as vehicle's radio characteristics. In [58], an analytical study has been done on connectivity and the following results are taken. An interested reader may refer to [58] for a more detailed discussion. Hereinafter, we study the connectivity in VANETs by evaluating the probability distribution and expectations of the following metrics:

1. *Platoon size*, which is defined as the number of vehicles in each spatial connected cluster (platoon) or, equivalently, the number of vehicles in the connected path from any given vehicle
2. *Connectivity distance*, which is defined as the length of the connected path from any given vehicle

The former is important because it shows how many vehicles can hear a vehicle in the safety applications and can have data exchange in the comfort applications. The latter metric is important because a larger connectivity distance leads to a larger announcement area for the safety applications and better accessibility to roadside equipment (e.g., Internet gateways) for the comfort applications.

In [58] it is proved that in the free-flow traffic phase, the distribution of intervehicle distance is exponential where its rate can be mapped to the traffic flow parameter (in the traffic theory). This result is also in agreement with the empirical study conducted in [59] for sparse traffic conditions. The interesting point about this work is that it expresses the above-mentioned connectivity metrics based on the fundamental parameters of the traffic theory (flow, speed, and density). Although the analytical discussion that is based on infinite server queues [60] is beyond the scope of this chapter, in the rest of the chapter we will bring forth most important results. In the following equations, R is vehicles' transmission range (m), λ is traffic flow (veh/h/lane), V is a random variable representing vehicles' speed, and N is the random variable representing platoon size.

- Platoon size: The tail probability of the platoon size (i.e., the probability that at least k vehicles are connected) is

$$P_N(k) = P(N \geq k) = [1 - \mathrm{e}^{-\lambda R E(1/V)}]^{k-1} \tag{13.8}$$

The expected value of the number of vehicles in each platoon is given by

$$E(N) = \frac{1}{\mathrm{e}^{-\lambda R E(1/V)}} \tag{13.9}$$

- Connectivity distance: Only the Laplace transform of tail probability of connectivity distance is obtained, which can only be inverted by numerical methods. For more explanation, refer to [58]. However, the average connectivity distance is given by the following explicit expression:

$$E(d) = \frac{1 - \mathrm{e}^{-\lambda R E(1/V)}}{\lambda E(1/V)\mathrm{e}^{-\lambda R E(1/V)}} \tag{13.10}$$

Using the obtained expression and stochastic ordering tools [61] (the details of which are beyond the scope of this chapter), one can describe the effects of various system parameters, including road traffic parameters (i.e., speed distribution and traffic flow) and the transmission range of vehicles, on the connectivity. From the above equations it is quite easy to see the effects of traffic flow and vehicles' transmission range on the connectivity. However, speed appears to be a random variable; thus, the effect of speed on the connectivity should be studied based on stochastic ordering techniques. In other words, to compare the effects of different speed scenarios on the connectivity, stochastic bounds can be presented. The details of stochastic ordering analysis can be found in [58]. However, in the following, we bring some numerical results aiming at pointing out some important findings.

First it should be noted that the following results hold for low-density traffic, which correspond to the free-flow traffic phase in Figure 13.1. In the free-flow state, the traffic flow is usually

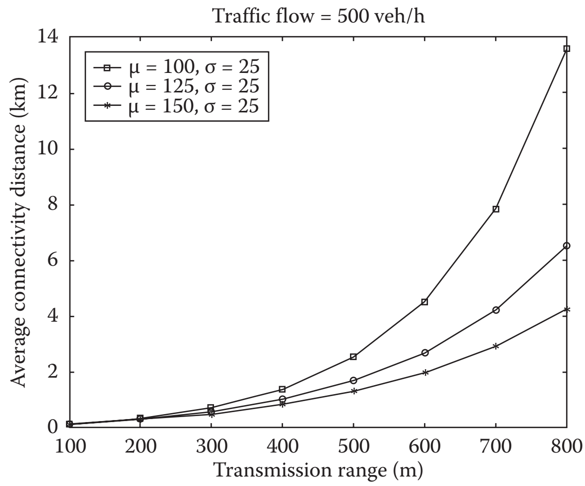


Figure 13.14 Effect of speed scenarios with similar variances and different means on the average connectivity distance. (From Yousefi, S., Altman, E., El-Azouzi, R., and Fathy, M., *IEEE Trans. Veh. Technol.*, 57(6), 3341–3356, 2008. With permission. © (2008) IEEE.)

considered to be below 1,000 veh/h/lane for freeways and below 500 veh/h/lane for other roads [5]. Moreover, although the proposed transmission range for the DSRC standard is 1,000 m [1,2], the current feasible range is about 300 m [14]. In the following figures, we provide results by taking the traffic flow values below 1,000 veh/h/lane and the transmission range values of up to 800 m. Furthermore, we assume that the vehicles' speed is normally distributed, which also holds in the free-flow state [5,62], and use some typical reported values. Furthermore, speed distribution is denoted by N(μ, σ) where μ and σ are the mean and standard deviation values, respectively.

a. If $\mu_1 > \mu_2$ and $\sigma_1 = \sigma_2$: As shown in Figure 13.14, the speed scenario with higher mean leads to a lower expected value of the connectivity distance. This trend also holds for the tail probability of the platoon size, the tail probability of the connectivity distance, and the average platoon size. The related figures are dropped due to space limitation. Consequently if we decrease the mean value of speed distribution, then the connectivity is improved provided that the variance of speed distribution is unchanged.
b. If $\mu_1 = \mu_2$ and $\sigma_1 < \sigma_2$: As shown in Figure 13.15, the traffic's speed with higher variance leads to a higher average connectivity distance. This trend also holds for the tail probability of the platoon size, the tail probability of the connectivity distance, and the average platoon size. The related figures are dropped due to space limitation. Here an interesting result is obtained, which may be in disagreement with our previous belief: If the variance of the speed's distribution is increased, then, provided that the average speed remains fixed, the connectivity is improved. The condition of fixed mean of speed is critical here. One can justify this result by that when the average speed is fixed, an increasing variance that causes more variability may help intermittent connectivity.

13.9.1 Connectivity of VANETs in the Presence of RSUs

In the previous section, we studied connectivity in a pure VANET where all nodes are moving vehicles. However, in real implementations, the pure ad hoc network coexists with fixed RSUs to

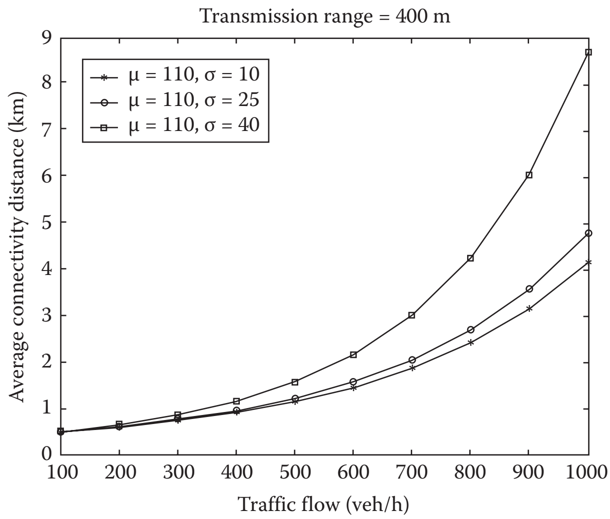


Figure 13.15 Effect of speed scenarios with similar means and different variances on the average connectivity distance. (From Yousefi, S., Altman, E., El-Azouzi, R., and Fathy, M., *IEEE Trans. Veh. Technol.*, 57(6), 3341–3356, 2008. With permission. © (2008) IEEE.)

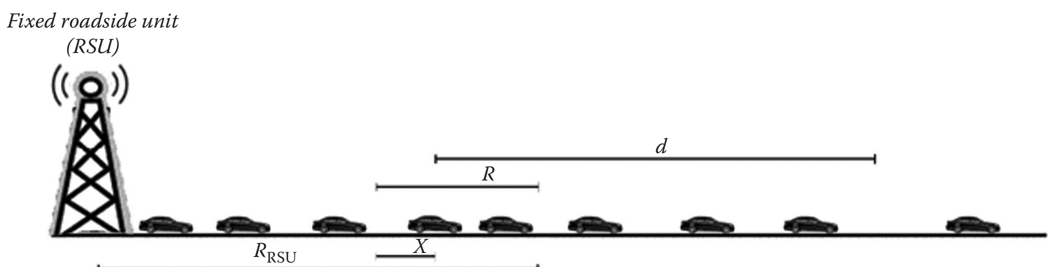


Figure 13.16 Connectivity of VANETs in the presence of RSUs. (From Yousefi, S., Altman, E., El-Azouzi, R., and Fathy. M., *Computer Communications*, vol. 31, no. 9, pp. 1653–1659, 2009. With permission.)

make a hybrid VANET. In particular, the comfort applications are relied on such RSUs to offer services to the vehicles on roads. Therefore, studying connectivity in the presence of RSUs is practically important. It is quite reasonable to assume that an RSU has a larger transmission range than an ordinary vehicle, although the following discussion is not restricted to that assumption. Let R_{RSU} and R_1 be the transmission range of the RSU and of all vehicles, respectively. Let d_{RSU} be the random variable representing the distance through which the RSU can communicate (the connectivity distance from the RSU).

As shown in Figure 13.16, this distance can be obtained by taking into account two independent distances: (1) the distance covered by the RSU with its own transmission range and (2) the distance covered by the pure ad hoc network formed between vehicles. Consider the car whose location is the smallest among all those who are larger than $R_{RSU} - R_1$, and let X be its distance from that point. If $X > R_1$, then this car is not connected to the RSU and the connectivity distance is R_{RSU}. If $X \leq R_1$, then at point $R_{RSU} - R_1 + X$, d is the new connectivity distance. The aforementioned problem has been studied in [63]. Opposed to the case of pure VANETs, no expression for tail probabilities has been obtained. However, for the average connectivity distance, the following expression is presented:

$$\bar{d}_{RSU} = R_{RSU} - R + (\hat{d} + \frac{1}{\xi})(1 - e^{-\xi R}) \tag{13.11}$$

where $\bar{d}_{RSU}$ is the average connectivity distance from the RSU, $\hat{d}$ is the average connectivity distance in a pure ad hoc network (stated in Equation 13.10), and $\xi = \lambda E(1/V)$. Moreover, the following expression has been presented for the average number of vehicles with which the RSU can communicate (in each direction):

$$\bar{N}_{RSU} = R_{RSU}\xi + \hat{N}(1 - e^{-\xi R}) - e^{-\xi R} + 1 \tag{13.12}$$

where $\bar{N}_{RSU}$ is the average connectivity distance in the presence of the RSU and $\hat{N}$ is the average platoon size in a pure ad hoc network (stated in Equation 13.9).

As an open research problem, one can study the variability of connectivity metrics in the course of time. It should be noted that in the discussion above and almost all other works in the literature, a snapshot viewpoint of the network is considered. In other words, it is implicitly assumed that the communication is instantaneous. However, one may intend to study connectivity variability during a long-lasting communication. For this purpose it is necessary to obtain analytical expressions for connectivity duration, which is very beneficial in designing a VANET protocol. Another important problem of connectivity, as mentioned above, is connectivity in the presence of radio and channel effects such as fading and shadowing. Furthermore, in the case of hybrid VANETs, one may be interested in obtaining optimum number of RSUs and their distance distribution in order to provide an acceptable connectivity. The mentioned problem is very critical in the effective design of future VANETs.

13.10 Data Dissemination in VANETs

Data dissemination is referred to as the process of routing and forwarding information originated from a vehicle termed as the source to another vehicle termed as the destination. In the literature, terms "dissemination," "routing," and "forwarding" are employed interchangeably. Data dissemination mainly involves unicast forwarding in order to eliminate packet duplication due to overhead concerns. The main goal of message broadcasting is to enhance the achievable safety of vehicular traffic; however, dissemination mechanisms are aimed at facilitating future emerging traffic management solutions and comfort applications expected by different industrial and academic bodies. While safety applications mostly need local broadcast connectivity, it is expected that some emerging scenarios developed for ITSs would benefit from unicast communication over a multihop connectivity [64].

Dissemination techniques applicable in VANETs are classified into two broad categories based on their specific characteristics: topology-based and geographic (or position-based) routing. In the following, an overview of important features of these routing approaches is given and the most popular routing protocols proposed for VANETs by research bodies are introduced and discussed in more detail. It is important to note that some of the routing protocols mentioned hereafter are used only as a benchmark for comparison purposes and may not be properly applicable in vehicular networks.

13.10.1 Topology-Based Routing

Topology-based routing protocols work based on the concept of links and use links' information to forward data/warning packets. Depending on whether route discovery is involved in the routing process, these routing protocols can be classified into reactive or on-demand and proactive or table-driven. In proactive routing, control packets are periodically propagated in the network to acquire and maintain links existing between nodes in pair. As a part of the routing process, a table is constructed such that each entry in the table represents the next hop toward a potential destination. In table-driven routing schemes, the source node should maintain unused routes. Maintenance of unused routes utilizes a significant amount of bandwidth, which is undesired in vehicular networks due to high mobility and frequently changing network topology. A representative example of proactive routing protocols is fisheye state routing [65], which maintains a network map at each node and propagates link state updates to neighbor nodes.

In reactive routing protocols, upon receiving a packet from the application layer a node initiate route discovery to find a path to the intended destination. Path discovery is usually conducted by means of a query–reply procedure implemented in the form of route request (RREQ) and route reply (RREP) messages. When a path is discovered, it will be used by communication parties and will be maintained as long as it is used. If due to any reason a path failed, another route discovery procedure is triggered. Among various topology-based routing protocols, a few of them have been applied to vehicular networks. These protocols include Ad hoc On Demand Distance Vector (AODV) [66], Ad hoc On Demand Distance Vector - Preferred Group Broadcasting (AODV-PHB) [67], Dynamic Source Routing (DSR) [68], PRediction based AODV (PRAODV), and PRediction based AODV - Maximum predicted value (PRAODV-M) [69]. In AODV, upon receiving a routing query, an intermediate node records the address of a sender node and upon receiving in the destination a reply packet is sent back to the sender through the path that was taken by the query. During propagation of RREP, each intermediate node will identify and record the next hop, thereby creating a forwarding path. The main drawback of AODV if applied in VANETs is the delay associated with the route discovery procedure. Furthermore, as route discovery control packets are broadcasted in the network, packet collisions due to broadcast storm are inevitable. In addition, the routes created by AODV can break very frequently due to the dynamic nature of mobility involved. To suppress the effect of frequent route breakage and thus increasing the routing performance, some enhancement mechanisms have been proposed. In [67], a new broadcasting method referred to as preferred group broadcast (PGB) that aims at mitigating the broadcast overhead and route instability associated with AODV is introduced. According to the characteristics of the received signal, each node determines whether it can be a member of the preferred group. Among member vehicles, only one vehicle with the highest signal quality will finally forward the route query packet. In urban vehicular networks where interference due to the presence of obstacles is a common adverse phenomenon, the application of AODV-PGB outperforms AODV in that it suppresses interference effects to some extent [67]. However, in case preferred group is empty or because the vehicle chosen as the forwarder is not necessarily the closest node to the destination, delivery latency imposed by this protocol can be potentially high. PRAODV and PRAODV-M are prediction-based extensions to AODV. In these protocols, speed and location information of nodes is employed to predict the links' lifetimes. PRAODV constructs a new alternate route before the end of the estimated lifetime while AODV does it until route failure happens. PRAODV-M selects the maximum predicted lifetime path among multiple route options instead of selecting the shortest path in AODV and PRAODV. There are other modifications to AODV, which are worth mentioning here. In [70], AODV is modified to forward the RREQs only within the zone of relevance (ZOR). The basic idea is the same as the location-aided routing (LAR) [71]. The ZOR is usually specified as a rectangular or circular range, and it is determined by the particular application [72].

DSR is similar to AODV in that it forms a route on-demand when a transmitting computer requests one. However, it uses source routing instead of relying on the routing table at each intermediate device. Determining source routes requires accumulating the address of each device between the source and the destination during route discovery. The accumulated path information is cached by nodes processing the route discovery packets. The learned paths are used to route packets. To accomplish source routing, the routed packets contain the address of each node the packet will traverse. This may result in high overhead for long paths or large addresses, such as IPv6. To avoid using source routing, DSR optionally defines a flow id option that allows packets to be forwarded on a hop-by-hop basis. It is worth mentioning that some modifications of DSR with a focus on security issues have been proposed recently. Ariadne [73] extends DSR by security functions using symmetric cryptography. The authors suggest any of these three schemes: shared secrets between each pair of nodes, shared secrets between communication nodes combined with broadcast authentication, or digital signatures. Although the latter scheme does not use symmetric cryptography, it is also considered as an option due to its high reliability, but not as the preferred option because of high processing requirements.

The disadvantage of DSR is that the route maintenance mechanism does not locally repair a broken link. Stale route cache information could also result in inconsistencies during the route reconstruction phase. The connection setup delay is higher than in table-driven protocols. Even though the protocol performs well in static and low-mobility environments, the performance degrades rapidly with increasing mobility. Also, considerable routing overhead is involved due to the source-routing mechanism employed in DSR and this routing overhead is directly proportional to the path length.

13.10.2 Geographic (Position-Based) Routing

In position-based routing protocols, forwarding decision is mainly made according to the position of the destination as well as the position of nodes in the radio range of the source node. This implies that the position of the destination should be available to the source node prior to packet transmission. Furthermore, each 1-hop neighbor requires its position information at any given time instance in order to inform the immediate previous forwarder(s) of its position or use its own position to decide whether or not it is qualified to participate in the forwarding process. In geographic routing, it is assumed that nodes identify their current positions by means of GPS that is already available in existing transportation systems and is deemed to be ubiquitous in near future. Moreover, availability of navigation and location services [74] enables a source node to identify the position of the destination node.

Position-based routing techniques can be further classified based on specific strategies and indicators used by routing protocols [64]:

- DTN vs. non-DTN: A routing scheme is categorized as a DTN (delay tolerant network) routing protocol if the intermittent connectivity of a vehicular network is presumed in a routing protocol and accordingly forwarding mechanism is designed in a way that forwarding process continues in case of network fragmentation. On the contrary, in non-DTN routing protocols, a network is assumed to be connected by default. In case forwarding process encounters network fragmentation, a reactive recovery process is enabled or the packet is simply dropped.
- Beacon-based vs. non-beacon-based: If a routing strategy uses beacon messages to gather information about 1-hop or 2-hop neighbors, it is referred to as beacon-based routing. Beacons usually play two roles in routing and forwarding process. They are used either to locate the closest neighbors to the destination or to identify anchor nodes (e.g., vehicles locating on junctions or on road turning points). The latter is usually performed via 2-hop beaconing.
- Overlay vs. non-overlay: Some routing protocols rely on anchor nodes located in specific locations, such as junctions in urban environment, to make decision to which direction (or road segment) packets should be routed. Such routing strategies are classified as overlay routing. A key task in overlay routing is to locate and identify overlay nodes.

In the following, a number of well-known position-based routing schemes are investigated. This investigation will be concluded with a discussion on open issues and challenges of these routing protocols when employed in VANETs.

Vehicle assisted data delivery (VADD) [75] is a beacon-based and DTN routing protocol aiming at packet forwarding in sparsely connected vehicular networks. In VADD, it is assumed that vehicles find their neighbors through beacon messages. It is also assumed that vehicles are equipped with preloaded digital maps, which provide street-level map and traffic statistics such as traffic density and vehicle speed on roads at different times of the day. Digital maps are used in VADD to model delay associated with road segments. Parameters such as road density, average vehicle velocity, and road distance are employed to model road delay. This facilitates optimal path selection by nodes located in junctions. Forwarding decision is then made by choosing next forwarding node according to different strategies proposed in VADD. In location first probe (L-VADD) strategy, next forwarding node is the one closest to the selected forwarding path. Direction first probe (D-VADD) simply chooses a next forwarding node driving toward forwarding path. In hybrid strategy (H-VADD), a combination of two mentioned schemes is used for next forwarding node selection. After next forwarding hop is determined, it follows position-based strategy to further propagate the packet toward the destination. If network fragmentation is encountered, the current forwarding hop follows carry and forward strategy. According to [75], in light traffic conditions, VADD outperforms the Greedy Perimeter Stateless Routing (GPSR) [76] routing protocol in terms of delay and delivery ratio. However, performance of VADD in dense traffic conditions such as urban environment and in the presence of interference sources is not specified. Moreover, as mentioned, VADD relies on digital maps to model path delay. This imposes a delay overhead on the routing protocol as such maps should be downloaded and updated frequently through Internet access gateways. Alternative solutions with lower delay would be continuous path delay estimation by vehicles themselves or periodic dissemination of traffic conditions of roads by RSUs to nearby vehicles.

Geographical opportunistic routing (GeOpps) [77] is a DTN routing protocol that employs information provided by navigation systems installed onboard vehicles to opportunistically route data packets to a certain geographical location. GeOpps performs three subtasks to route a packet to the destination: (1) Neighbor vehicles that follow suggested routes to their driver's destination calculate the nearest point that they will get to the destination of the packet. (2) Afterward, they use the nearest point and their map in a utility function that expresses the minimum estimated time that this packet would need in order to reach its destination. (3) The vehicle that can deliver the packet quickly/closer to its destination becomes the next packet carrier. As GeOpps needs trajectory of neighbor vehicles to be available in the current forwarding vehicle, it may not be desirable from the security point of view.

GPSR [76] is a non-DTN, non-overlay, and beacon-based routing protocol. GPSR performs routing in two modes. Initially, it forwards packet in greedy fashion, meaning that among neighbors of a current forwarder the closest one is selected as the next hop to forward the packet. A node reaches a local maximum if it cannot find a neighbor closer than itself to the destination. In this case, GPSR triggers the recovery process and recovers from local maximum using a perimeter mode by means of the right-hand rule. If a node closer to the destination is not found in the perimeter mode, a face change (also called face routing) is performed. Upon finding a closer node to the destination, a greedy mode is enabled again until the packet is received in the destination. Operation of GPSR needs network graph to be planar. To fulfill this, GPSR uses some distributed algorithms to build planar graphs. Relative neighborhood graph [78] and Gabriel graph [79] are two planar graphs that are created in GPSR. The unit graph assumption is adopted in GPSR to create connected planar graphs. According to the unit graph assumption, two nodes are referred to as connected if their distance is less than a predetermined threshold; otherwise they are not connected. However, as in vehicular networks this assumption does not always hold due to the presence of obstacles and interference, applicability of GPSR is questionable [64]. Furthermore, the delay overhead imposed by GPSR in the greedy mode and the time needed to create planar graphs are not desirable in vehicular networks. Finally, in highly dynamic vehicular networks, positions of neighbors and destination change rapidly. This results in outdated position information in nodes currently deciding to forward the packet. In [67], an approach referred to as advanced greedy forwarding (AGF) is proposed as a solution to address this problem. Based on AGF, beacons are augmented with information reflecting dynamic behavior of vehicles. Information such as velocity vector (speed and direction) of each vehicle is included in beacons. Knowing velocity vector of neighbors, each vehicle can estimate their current locations. Moreover, each vehicle can estimate the current position of the destination. This strategy, although being preferable to GPSR, has some drawbacks. First, it does not work for vehicles changing their directions in junctions. Second, impacts of acceleration and deceleration are not considered in AGF. In [80], Schnaufer et al. proposed position-based routing with distance vector recovery as an alternative to the perimeter mode in GPSR when a transmitted packet reaches a local maximum. Upon receiving a packet from a vehicle currently at local maximum, the recipient vehicle checks if it is closer to the destination than the vehicle at local maximum. If it is not, then the packet is broadcasted again. If the recipient is closer to the destination, a reply packet is sent back to the vehicle at local maximum. Intermediate nodes will learn the previous nodes from which they received the reply packet. This enables the vehicle at local maximum to transmit through reply path. This solution eliminates the need for the creation of a planar graph as in GPSR. However, it inherits the drawbacks of AODV such as delay overhead as a result of the route discovery procedure. Greedy routing with abstract neighbor table (GRANT) [81] is another approach belonging to the GPSR family of protocols. The core idea of GRANT is to predict local maximum based on x-hop neighbor information. To avoid overhead imposed by x-hop beaconing, the plane is divided into areas and a single node is designated per area for beaconing purposes. The metric proposed in GRANT to select the next forwarding node is measured by the multiplication of distance between x-hop node and destination, distance between x-hop node and current forwarding node, and charge (or cost) per hop.

A slightly different category of geographic routing protocols adopts an overlay design. In these protocols, anchor points, i.e., nodes located in junctions, and turning points play critical roles in routing and forwarding process. Therefore, a key task in overlay protocols is to find anchor points and augment vehicles locating in anchor points with link state and traffic information of road segments connected to these points. Strategies used to identify anchor points fall into two categories. They use either a topological map or dynamic algorithms to determine anchor points. In what follows, a number of geographic overlay routing protocols are investigated and discussed in more detail.

One of the well-known geographic overlay protocols aiming at the elimination of the need for graph planarization is greedy perimeter coordinator routing (GPCR) [83]. In this scheme, junctions are identified by means of heuristic algorithms and are used as graph vertices. The resultant graph is naturally planar, and hence the planarization process is skipped. In case of encountering a local maximum, recovery will be performed by representative vehicles located on junctions. Packets are forwarded in greedy fashion along streets and stops whenever they reach a junction, where they are decided on which direction to proceed. GPCR differs from GPSR in that it does not need graph planarization.This may result in significant time saving in GPCR compared to GPSR. This is due to the fact that in GPSR, the network graph is formed by vehicles and not by junctions. Considering the fact that vehicles' mobility causes the network topology and hence the graph shape to change, a palanrization process must be invoked to create a new planar graph corresponding to the current network topology.

Geographical source routing (GSR) [83] uses a street map to identify junctions. Using such a map, GSR builds a graph with road segments indicating graph edges as well as junctions representing vertices. A sequence of junctions represents a path, and Dijkstra's shortest-path algorithm is employed to find shortest paths. When such a path is found, packets are forwarded in greedy fashion between junctions comprising the path. Unlike GSR, A-STAR [84] is a connectivity-aware routing approach that eliminates those anchor points in the shortest path that are not located on a connected path. Similar to GSR, A-STAR adopts the anchor-based routing approach with street awareness. The term "street awareness" is preferred over "spatial awareness" to describe more precisely the use of street map information in the routing scheme for anchor path computation [84], that is, using a street map to compute the sequence of junctions (anchors) through which a packet must pass to reach its destination. Unlike GSR, A-STAR computes the anchor paths with traffic awareness. "Traffic" herein refers to vehicular traffic, including cars, buses, and other roadway vehicles. A possible drawback of A-STAR is its dependence on RSUs that impose an overhead delay on routing protocols. In [85], an alternative solution referred to as street topology-based routing (STBR) is proposed to calculate connectivity of paths. In this approach, a representative node at each junction is responsible for tracking the connectivity status of road segments connected to the junction. This is performed by disseminating beacon messages by each representative vehicle on a junction to all other neighboring junctions' representatives. This strategy provides each representative vehicle in a junction with a 2-hop neighbor junctions' link information. Unlike GSR, Dijkstra's algorithm is not used to find the shortest path [64]. Instead, packets are geographically forwarded from street node (source) to junction, from junction to junction, and from junction to street node (destination). STBR has two major drawbacks: first, it does not specify any strategy when no junction makes progress toward the destination. Second, to build and maintain a neighbor table in each representative node, a significant number of beacons should be exchanged between junctions. This puts an excessive overhead on the routing protocol and wastes channel resources at the cost of safety applications.

To further enhance geographic routing protocols with connectivity awareness, a number of approaches have been proposed in the literature. In [86], Jerbi et al. proposed greedy traffic aware routing protocol (GyTAR). In GyTAR, it is assumed that each vehicle in the network knows its own position and current geographical position of the destination in order to make the routing decision. Moreover, it is assumed that each vehicle can determine the position of its neighboring junctions through preloaded digital maps, which provides a street-level map. It is also assumed that every vehicle is aware of the vehicular traffic (number of vehicles between two junctions). According to Jerbi et al., this information is provided by Infrastructure-Free Traffic Information. System (IFTIS): a decentralized mechanism for the estimation of traffic density in a road traffic network. In GyTAR, the different junctions the packet has to traverse in order to reach the destination are chosen dynamically and one by one, considering both vehicular traffic variation and distance to the destination: when selecting the next destination junction, a node (the sending vehicle or an intermediate vehicle in a junction) looks for the position of the neighboring junctions using the map. A score is given to each junction considering the traffic density and the geometric distance to the destination. The best destination junction (the junction with the highest score) is the one that is geographically closest to the destination vehicle and has the highest vehicular traffic. Landmark overlays for urban vehicular routing environment (LOUVRE) [87] is slightly different in the way it estimates connectivity. Instead of relying on RSUs, LOUVRE estimates traffic density in a peer-to-peer fashion by means of beacon messages exchanged by vehicles to their neighbors. Above a threshold density determined by road length and radio communication range, a road is said to be connected. The drawback associated with both GyTAR and LOUVRE is that vehicle density is not a suitable metric for connectivity measurement unless vehicles are distributed uniformly along the road under investigation. This assumption can be safely applied to highway scenario to some extent but in urban scenario such an assumption is not realistic. Connectivity-aware routing (CAR) [67] addresses connectivity from a different viewpoint. CAR employs AGF [80] to predict mobility of the destination and vehicles that were the neighbors of the current forwarding vehicle. This way, without too frequent beaconing and triggering location service, a vehicle can adaptively keep locations of its neighbors and the destination. This enables forwarding vehicle to have fresh information about its local connectivity. CAR is similar to AODV in that it uses a similar approach for route discovery. However, route discovery in CAR differs from that in AODV in two ways: first, a limited broadcast strategy is implemented by means of PGB [67]. Second, only anchor points (located on junctions) are reported in the reply packet. By receiving the information of anchor points within the reply packet, the source node employs AGF to forward packets explicitly to those anchor points and implicitly to the destination.

Contention-based forwarding (CBF) [88] adopts a different strategy than those protocols mentioned before in that it does not rely on beaconing. Instead, CBF uses contention to implicitly select the next hop in the communication path. Each potential forwarder computes the time t it must wait before forwarding the packet depending on its suitability, i.e., its progress toward the destination defined as:

$$P(F,\ D,\ N) = \max\left\{0,\ \frac{\text{dist}(F,\ D) - \text{dist}(N,\ D)}{r_{\text{radio}}}\right\} \tag{13.13}$$

$$t(P) = \begin{cases} \max\{0,\ T(1-P)\}, & P > 0 \\ \infty, & \text{otherwise} \end{cases} \tag{13.14}$$

where P is the progress function depending on the positions of the last forwarder F, of the final destination node D of the packet, and of the receiving node N. The Euclidean distance between two positions is expressed as dist( ). r_{radio} denotes the maximum 1-hop distance toward the destination a message can travel and T defines the maximum contention time. $t(P)$ is the assigned waiting time to a node. Observe that CBF does not take into account the role of traffic density in the progress function P. This leads to actual forwarding progress to be less than the amount of progress estimated by (13.13). However, as CBF takes advantage of both geographic routing and opportunistic forwarding, it is categorized as a geo-opportunistic routing scheme. This family of protocols is more preferable in the presence of interference due to robustness of opportunistic forwarding against interference.

13.10.3 Open Issues

In addition to drawbacks identified for each routing protocol surveyed in previous sections, two other major challenges observable in all routing protocols are connectivity and interference awareness. In our terminology, interference is a by-product of at least two components: First, it is caused by static and dynamic physical objects such as buildings and vehicles in urban environments. High contention over channel access in high traffic densities such as queues built behind junctions or jams caused by accidents is considered as a second interference source. The latter is also caused by broadcast storm and hidden terminal effects and is intensified in dense traffic conditions. As a general fact, traffic density contributes to both interference types assuming that traffic density is proportional to packet transmission rate. This assumption is realistic in VANETs since, as specified in standard, all vehicles need to propagate beacon messages frequently.

In table-driven routing strategies due to high topology change in VANETs, the update rate of link states increases dramatically, which results in a high packet collision rate. Another source of collision is periodic link state exchange as specified by the protocol. In addition, as link state updates are exchanged only with neighbors and each node records only next-hop information toward a destination, a notion of end-to-end connectivity is not considered in table-driven protocols. When a packet fails to reach the destination, it is simply dropped and retransmitted, which in turn leads to delay overhead and wasteful bandwidth usage.

Delay associated with the route discovery procedure in reactive topology-based routing protocols hinders their applicability in VANETs. Furthermore, as route discovery control packets are broadcasted in the network, packet collisions due to broadcast storm are inevitable (AODV-PGB is an exception in that it limits the broadcast rate). In addition, as in VANETs the lifetime of connections is short, the routes created by reactive protocols are not stable. This causes the packets forwarded in predetermined routes to encounter route breakage due to network fragmentation or interference. Reactive protocols do not offer any strategy to predict route breakage dynamically and to handle packet forwarding when such incident occurs.

Geographic routing protocols deal with connectivity and interference in different ways. In DTN routing schemes such as epidemic, VADD, and GeOpps, a reactive strategy based on the store-carry-forward scheme is adopted when a forwarding node detects network fragmentation. These routing protocols ideally guarantee packet delivery at the cost of unbounded delay. Protocols in the GPSR family are similar to DTN protocols in that they react to network fragmentation only when it is detected during forwarding. However, instead of the store-carry-forward scheme, they rely on recovery schemes mainly implemented by perimeter traversal based on the right-hand rule. Based on whether or not a graph planarization procedure is required for a perimeter traversal purpose, protocols in the GPSR family adopt different strategy. As a general fact, graph planarization is not desired in VANETs due to its unit graph assumption. This invalid assumption makes protocols such as GPSR not robust against interference and less connectivity-aware owing to false link identification. On the contrary, overlay protocols such as GPCR perform routing on a natural planar graph composed of junctions and road segments. These protocols although being more promising in terms of robustness against environmental interference when they operate in the recovery mode, they do not propose an interference-aware forwarding strategy in greedy mode operation. A different class of geographic routing schemes is proactive in the way they deal with connectivity issues. GRANT, CAR, A-STAR, STBR, GyTAR, and LOUVRE are examples of this kind. Common to all of these protocols is rough estimation of traffic along the road segments and junctions and exploit it as a measure of connectivity. Traffic estimation mechanisms adopted in these protocols either are too simplistic or impose high overhead on the underlying network. A group of geographic routing protocols are neither reactive nor proactive and thus are not connectivity-aware. GSR and CBF are categorized in this group. An interesting advantage of CBF is its opportunistic forwarding strategy that makes it relatively robust against interference.

In conclusion, while routing protocols address interference and connectivity in VANETs to some extent, they sacrifice one to the advantage of another to achieve acceptable results for some proprietary traffic scenarios that by no means are extendable to various scenarios existing simultaneously in urban environments, for instance. In the best case the existing routing schemes predict connectivity prior to data forwarding, although the measurement strategies are not accurate or time-efficient. Thus, a fundamental analytical and experimental study is needed to investigate interference and intermittent connectivity of VANETs and the challenges caused by these issues especially in urban scenarios. A further step would be the application of the results of such a study to devise new data and message dissemination schemes.

13.11 Broadcast in VANETs

Unlike comfort applications, event-driven safety applications require that warning messages be broadcasted to a large number of vehicles instead of disseminating to a single vehicle or a fixed RSU. Message flooding is the most common scheme employed for message propagation in these applications. However, an immediate drawback of flooding approach is broadcast storm phenomenon that results in traffic overwhelming due to blind message propagation by vehicles acting as relays in multihop communications. The consequences of such a phenomenon are exacerbated in dense traffic conditions as the competition over channel access increases dramatically, which in turn leads to high packet collisions. An obvious result of packet collision is the low packet delivery ratio, implying for some vehicles not to receive the warning message at all. Considering that the delivery of warning messages is highly demanded in the case of emergency incidents, existing flooding-based approaches tend to reduce collisions by means of suppressing broadcast storm phenomenon. Broadcast approaches with flooding suppression can be categorized into four different classes [89] as described below.

13.11.1 Geographical-Limited Broadcasting

Geographical broadcasting (geocast) is a type of traditional multicasting. The difference is that geographical broadcasting is limited to vehicles spreading over a specific geographical area (i.e., geocast region). More specifically, in case of an emergency incident, only a subset of vehicles driving in the vicinity of the incident site are targeted as warning message recipients. Such vehicles are termed "geocast group." A geocast group is dynamic in that vehicles leaving the geocast region are removed from the group while vehicles driving into the geocast region at a given time become members of the group. In [90], Bachir and Benslimane proposed a novel geocast protocol for broadcasting warning messages based on their associated relevance to the current location of vehicles. This protocol aims at delivering messages to those vehicles approaching an accident site. Those irrelevant vehicles far from the accident location drop warning messages they receive, while relevant vehicles participate in rebroadcasting warning messages. Although the geocast approach reduces broadcasting to a limited region, still the problem of the broadcast storm in the geocast region remains unsolved.

13.11.2 Priority-Based Multihop Broadcast

Time critical warning messages are the most influenced by the broadcast storm phenomenon. One approach is to give higher priority to those nodes that need to propagate warning messages than those nodes that are transmitting periodic beacons or data packets. This approach has been introduced in [91], where an algorithm for classifying different nodes based on the type of message they intend to transmit is proposed. Then a scheduling algorithm is devised to transmit messages based on their holders' priorities. It is important to note that this approach does not address the broadcast storm problem; instead, the impacts of this problem are mitigated to the benefit of high-priority event-driven applications.

13.11.3 Distance-Based Multihop Broadcast

Distance-based approaches mainly aim at broadcast storm suppression by giving higher opportunity to those nodes farther from the current transmitter as the candidate next-hops participating in the rebroadcasting process. Ideas pursuing this approach fall into two main categories: (1) only the farthest node from the current sender rebroadcasts the warning message [92], (2) a group of vehicles situated in the broadcast range hearing the transmitted message participate in rebroadcasting according to a priority scheme. Priorities are given to vehicles based on their distance from the transmitter (as opposed to greedy geographic routing where the closest node to the destination is selected as the next hop). In [93,94], three different mechanisms are proposed based on the second approach: weighted p-persistence, slotted 1-persistence, and slotted p-persistence broadcasting.

Weighted p-persistence and slotted p-persistence are known as variations of gossip-based broadcasting approach, also referred to as probabilistic broadcasting [95], where vehicles receiving a transmitted packet rebroadcast it with some probability p. In weighted p-persistence, the broadcast probability of a vehicle driving in the broadcast range of the transmitter is determined according to the distance of this vehicle to the current transmitter. More specifically, upon reception of a packet in node j from node i, the forwarding probability p_{ij} is calculated as D_{ij}/R, where D_{ij} is the distance of node j from node i and R is the average transmission range. Before rebroadcasting, node j checks the packet ID and rebroadcasts it with the probability p_{ij} if it is the first time this packet is received by node j. The slotted p-persistence mechanism follows a slightly different approach. In this approach, the forwarding probability p is known *a priori* and is not calculated per-packet. Moreover, each recipient vehicle rebroadcasts with probability p at its assigned time slot if it is the first time it receives the packet and also has not received any duplicate packet before its assigned time slot. The longer the distance from the transmitter, the shorter is the time a recipient vehicle waits for rebroadcasting.

In the slotted 1-persistence mechanism, each recipient vehicle in the transmission range of the sender calculates its time slot in a way similar to that of the slotted p-persistence mechanism. However, it rebroadcasts with probability 1 if it is the first time it receives the packet and also has not received any duplicate packet before its assigned time slot. If packet delivery latency and penetration rate are of higher importance to safety application as compared with packet loss ratio, the slotted 1-persistence mechanism is preferred over other mechanisms. However, slotted p-persistence is more reliable from the packet loss point of view as long as the choice of p as a predetermined design factor is made carefully.

Another class of broadcasting schemes has been proposed in the literature based on the epidemic routing approach. These schemes differ from aforementioned broadcasting mechanisms in that messages are flooded network-wide to be hopefully delivered to a single destination instead of all vehicles or a group of them. Epidemic-based approaches can be categorized as unicast forwarding/routing techniques in which message communication occurs pairwise; i.e., messages are originated by a single sender and are targeted to a single destination. However, as already mentioned, the way they propagate messages is referred to as broadcasting. Epidemic-based message broadcasting is also classified as a type of delay-tolerant forwarding methods that work on the basis of the store-carry-forward scheme. The intention behind epidemic-based broadcasting is to cope with packet forwarding challenges arisen by frequent disconnection phenomenon in vehicular networks. To acquire a thorough insight into epidemic-based packet broadcasting, some well-known approaches and their derivations are investigated as follows.

13.11.4 Epidemic-Based Packet Routing Techniques

Epidemic routing [96] mimics the way an infectious disease spreads through direct contact in a population. If the disease is highly infectious and the individual contact frequencies are high, it is highly probable that the disease will spread through the entire population [89]. In a similar way, epidemic routing leads to all vehicles receiving a copy of the transmitted message with high probability; hence, any single destination targeted for the message will finally have the message with high probability. Basic epidemic routing is conducted in two phases: The first phase is initiated when two vehicles make their first contact. During this phase, vehicles exchange their message summary vectors containing the message IDs they have already received. In the second phase, contacting vehicles exchange new messages not being received previously. Each message has a time to live (TTL) field to restrict the number of contacts during which it can be exchanged. When a vehicle receives a message with TTL = 0, it is allowed to be exchanged only with the destination.

The apparent drawback of basic epidemic routing is flooding potentially the whole network in order to deliver a message to a single destination. In [97], the spray-and-wait approach is proposed to restrict the total number of broadcasted copies of the same message to a predetermined number L. In the spray phase, L copies of the message are forwarded to L distinct relays by the source vehicle and other receiving vehicles. In the wait phase, only direct transmission is allowed; i.e., relay nodes holding the message are allowed only to forward the message to the destination vehicle as soon as they contact. Restricting the number of message forwarding instances suppresses the negative impacts of the broadcast storm. Moreover, the spray-and-wait mechanism is scalable in the sense that with the increase in the number of vehicles (or equivalently traffic density), the number L of message copies is not needed to be increased in order to retain the same performance level achievable with a lower number of vehicles [89], i.e., when network is sparse. Despite positive aspects of the spray-and-wait approach, there is always a risk of unbounded delay as the message holder(s) may not ever have a contact with the destination vehicle during the wait phase.

To enhance epidemic routing further, Lindgren et al. [98] introduced PROPHET, a new epidemic-based forwarding mechanism targeted for delay-tolerant applications in vehicular environment. The key idea of PROPHET is delivery estimation made by each vehicle and represents the chance of message delivery from a typical vehicle to any other potential destination vehicle in the network. Delivery estimation is expressed in terms of delivery probability and calculated based on the contact history of a vehicle with other vehicles and updated upon any new contact of vehicles. According to Lindgren et al., the intuition behind PROPHET is that vehicle mobility in vehicular networks is not entirely random and vehicles tend to visit some locations more often or vehicles visiting one another in the past are more likely to have contacts in future. When nodes A and B contact, they initially exchange their message summary as well as delivery probability vectors and update their own delivery probability vectors according to the new information acquired during this contact. If vehicle A realizes that vehicle B has some messages for which it has higher delivery probability, then vehicle A chooses and transfer those messages for later delivery to the intended destination specified by vehicle B.

Another approach used for delivery estimation different from what is employed in PROPHET is based on virtual Euclidean mobility pattern space referred to as MobySpace [99]. According to MobySpace, messages should be forwarded to a next-hop node that shows a mobility pattern similar to that of the destination node. This approach has two drawbacks: First, vehicles must have a stable mobility pattern in order for MobySpace to be efficient [89]. Second, a similar mobility pattern in spatial dimension does not necessarily mean frequent contacts of vehicles. Mobility patterns should be similar in both spatial–temporal dimensions for rendering high message forwarding performance in MobySpace.

13.11.5 Open Issues

Broadcast storm as the major challenge of packet broadcasting in vehicular networks still stands without being fully solved. Approaches proposed to address this challenge either suppress it to a limited extent or lose some performance indicators such as delivery latency when they aim at resolving broadcast storm significantly. In geographic-oriented message broadcasting mechanism, although the impact of broadcast storm is reduced to a limited region rather than the whole network, still packet collisions and blind usage of transmission resources unavoidable in the geocast region targeted for message propagation. Priority-based broadcast techniques sacrifice data packets and beacon messages to the benefit of time critical messages. Besides, scalability of these techniques is questionable when the number of time critical messages increases in the network. Distance-based broadcast mechanism works well when traffic density is relatively low. In high-traffic-density conditions, there will be many nodes with identical or nearly equal forwarding probability or equally assigned time slot since these parameters are calculated according to the distance of vehicles to the message transmitter. Furthermore, in the slotted p-persistence broadcast mechanism, the choice of the parameter p, which plays a key role in the ultimate performance of broadcasting scheme, is assumed *a priori* for each vehicle. This imposes another challenge to the applicability of this mechanism. As a general fact, network connectivity is ignored in all broadcasting schemes as they assume that event-driven alarm messages are not needed to be delivered to the isolated regions and locations far from the incident location. Whether such assumption always holds is arguable as it is desirable to inform vehicles (perhaps far from the incident location) to proactively select alternative routes and avoid traffic jams caused by accidents.

Apart from basic epidemic routing, in most of the delay-tolerant broadcasting approaches the broadcast storm challenge is addressed remarkably and thereby significant improvement is achieved. However, in almost all of these mechanisms high latency is unavoidable and in some cases latency may be unbounded. For time critical alarm messages and real-time data packet dissemination, such mechanisms are not applicable. However, as a strong feature, epidemic-based forwarding and its associated variations are robust against intermittent connectivity in vehicular networks.

13.12 WiMAX in Vehicular Networks

Due to a recent surge of broadband wireless access, WiMAX has been attracting much attention from both industry and academic communities. The early proposal of WiMAX was based on IEEE 802.16-2004 (also called IEEE.802.16d), which supports both LOS (line of sight) and non-LOS for fixed nodes [100]. However, later in the framework of IEEE 802.16e (also called mobile WiMAX) [101], the support of mobility is added. The IEEE 802.16 standard defines a mesh operating mode along with a centralized mode called PMP (point to multipoint). In the former, data traffic occurs directly between subscriber station (SS) nodes; however, in the latter, data traffic should be handled by a centralized node called base station.

In general, WiMAX can be a potential candidate to be used in the vehicular network due its large transmission range and support of QoS. Actually the MAC layer of WiMAX is deterministic Time Division Multiple Access (TDMA)-like (as opposed to stochastic and contention-based nature of CSMA/CA of IEEE 802.11p). This is quite beneficial in avoiding MAC layer collision, in particular for beacon-based and alarm-based safety applications, which in turn leads to a higher safety level. Furthermore, WiMAX substantiates a class-based QoS support, which is very advantageous for comfort applications as well. The current QoS classes [100] include unsolicited grant service, real-time polling service, extended real-time polling service, non-real-time polling service, and best effort, which can be assigned for different kinds of applications, including safety and comfort applications.

It is expected that WiMAX in the PMP mode can be easily used for V2I scenarios. This issue has been studied in [102], and the preliminary results show that WiMAX offers larger coverage (a few kilometers), acceptable bandwidth, and even lower delay. Therefore, by using fewer RSUs the cost of network deployment is decreased noticeably. In this case the cost of base stations of WiMAX is a concern, which is much higher than that of IEEE 802.11p-based RSUs. However, as Ge et al. [103] suggested, one can invoke IEEE 802.16j, which is aimed at supporting multi-hop relaying. In other words, by taking advantage of relay nodes the cost of implementation of WiMAX is reduced. Another middle-ground approach is to make use of integrated IEEE 802.11p and IEEE 802.16 standards for achieving both high data rate and high coverage area, as suggested in [104]. It should be noted that the coverage area of wireless technologies for highway and urban scenarios not only depends on the coverage of the corresponding technology but also on other factors including number of vehicles, environment obstacles, and their service demand. An example of such a computation is provided in [105]. Depending on the aforementioned conditions, the coverage range of WiMAX is in the range of a few kilometers and that of IEEE 802.11p is in the range of a few hundred meters.

When it comes to life safety application, the view of WiMAX is not that much clear. First, WiMAX should operate in the mesh (ad hoc) mode due to the need of V2V communication, which is not supported in the current mobile WiMAX standard. Second, WiMAX is a connection-oriented MAC layer; thus, for each message transmission, several steps should be followed until a connection is established. This is not in favor of safety applications due to the fact that safety messages (in particular alarm safety messages) are issued in response to an unexpected event for which there is no previous intention of message transmission. Therefore, the time needed to set up the connection may violate timeliness requirement of safety applications.

The final point here is that even if the above ideas are realized, a vehicle has to support both mesh mode (for safety applications) and PMP and relay modes (for comfort applications) of WiMAX. However, the possibility and efficiency of such a solution should be investigated due to the substantial difference between operation and protocols of these two modes.

13.13 Current Status and Future Trends

Vehicular networks have motivated joint cooperation between scientific and industrial bodies in the recent decade. During these years the view on VANETs has changed slightly as depicted by the feedbacks taken from prototyped industrial projects. Currently, the ambitious view of automatic driving is replaced by driver-assistant safety applications because it seems that with current DSRC standards and technology it takes a relatively long time until fully automatic driving is substantiated. The main reason is that automatic driving, by its nature, demands very high performance and QoS metrics to be satisfied. Another major motivation for VANETs research and deployment will be comfort applications. Due to their business profit and lighter QoS requirements, comfort applications can be potentially very promising in the future. For safety applications, V2V communication is primordial, but for comfort applications, both V2V and V2I communications are required. The current DSRC standard, which is based on the IEEE 802.11p MAC layer, may remain *de facto* standard for V2V communications. But it seems that the current trend is toward using the IEEE 802.16e standard (also called mobile WiMAX) or another long-ranged/high-bandwidth wireless standard for V2I communications as a complementary or replacing technology.

In this chapter, several challenging issues with VANETs have been introduced and related solutions are discussed briefly. This work can be considered as an updation and complementary to [106]. Table 13.2 summarizes the current status and future trends discussed in this chapter.

Table 13.2 Current Issues and Future Challenges in Vehicular Ad Hoc Networks

Vehicular Ad hoc Network: Challenging Issues	*Relevant Type of Application*	*Current Status*	*Future Trend*
Performance evaluation metrics (refer to Section 13.4)	Safety	• As ordinary networking scenarios (focused on average values)	• New metrics focused on safety requirements (e.g., worst-case vales)
	Comfort		• As ordinary networking scenarios
Simulation (refer to Section 13.5)	Safety and comfort	• Integrated off-line imulation	• Integrated co-simulation
Transport layer protocols (refer to Section 13.6)	Safety	• Using UDP	• UDP along with some application layer reliability support for unrepeatable safety messages
	Comfort	• Customized versions of TCP	• Customized versions of TCP • UDP along with FEC techniques
Vehicle to RSU communications (refer to Section 13.7)	Comfort	• Intra-RSU data scheduling • Single-class inter-RSU data dissemination	• Multiclass data distribution • Inter-RSU scheduling algorithms • Optimum placement of RSUs • Design of dissemination protocols
Beacon-based safety applications (refer to Section 13.8)	Safety	• Power control • Application level scheduling • Transmission interval control	• Adaptive power control • Adaptive application level scheduling • Dynamic transmission interval control
Connectivity (refer to Section 13.9)	Safety and comfort	• Study of steady-state connectivity in sparse traffic • Simplified analytical modeling (mostly hold for free-flow traffic phase)	• Study of connectivity duration • Effect of traffic parameter on connectivity • Connectivity of hybrid VANETs (both V2V and V2I) • Connectivity impairment due to channel and radio conditions • Study of intermittent connectivity

(Continued)

Table 13.2 (Continued) Current Issues and Future Challenges in Vehicular Ad Hoc Networks

Vehicular Ad hoc Network: Challenging Issues	*Relevant Type of Application*	*Current Status*	*Future Trend*
Data dissemination in VANETs (refer to Section 13.10)	Comfort	• Position-based greedy routing schemes • Selective forwarding • Routing recovery	• Hybrid DTN and non-DTN routing • Connectivity- and interference-aware routing and forwarding • Geographic-opportunistic routing schemes
Broadcast in VANETs (refer to Section 13.11)	Safety	• Message flooding • Geographical restricted broadcast • Node and packet prioritization	• Interference-ware broadcast • Broadcast adaptation based on safety application requirements
WiMAX in vehicular networks (refer to Section 13.12)	Safety	• At the starting points (the application is in doubt)	• Support of mesh and ad hoc mode of mobile WiMAX (IEEE 802.16e) (the current standard does not support)
	Comfort	• Preliminary research results show promises	• Invoking WiMAX for V2I applications • Implementation of joint DSRC/WiMAX infrastructure • Invoking WiMAX with relay nodes (IEEE 802.16j) to reduce the cost of implementation

For a more detailed discussion, please refer to related sections indicated in the table. It should be stressed that the challenges that should be addressed in VANETs directly depend on the application in mind (i.e., safety or comfort). This is because different types of applications have different QoS requirements.

Acknowledgment

The authors thank Maissam Asgari, Hamid Karimi, Hassan Nassiraei, and Masoud Rezayat (the MSc students of Urmia University) for their assistance in preparation of this chapter.

References

1. Fed. Commun. Comm., FCC 03-324. FCC Rep. Order, February 2004.
2. IEEE Standard 802.11p Draft Amendment. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Wireless Access in Vehicular Environments (WAVE), IEEE, 2005.
3. National Center for Statistics and Analysis. Traffic Safety Facts 2003, Report DOT HS 809 767. Washington, DC: National Highway Traffic Safety Administration, U.S. Department of Transportation, 2004.
4. C.J. Adler. Information dissemination in vehicular ad hoc networks. Diploma Thesis, University of Munich, Germany, 2006. Available (in German) at http://www.destatis.de/ (Accessed on June 2011).
5. R.P. Roess, E.S. Prassas, and W.R. McShane. *Traffic Engineering*, 3rd ed. Upper Saddle River, NJ: Pearson Prentice Hall, 2004.
6. H. Morimoto, M. Koizumi, H. Inoue, and K. Nitadori. AHS road-to-vehicle communication system. In *Proceedings of the IEEE International Conference on Intelligent Transportation Systems, Tokyo, Japan*, 1999, pp. 327–334.
7. O. Andrisano, M. Nakagawa, and R. Verdone. Intelligent transportation systems: the role of third generation mobile radio networks. *IEEE Communications Magazine*, vol. 38, no. 9, 2000, pp. 144–151.
8. COMeSafety. Available at http://www.comesafety.org/ (Accessed on June 2011).
9. COM2REACT. Available at http://www.com2react-project.org/ (Accessed on June 2011).
10. COOPERS. Available at http://www.coopers-ip.eu/ (Accessed on June 2011).
11. CVIS. Available at http://www.cvisproject.org/ (Accessed on June 2011).
12. Intelligent Transport System. Cooperative intersection collision avoidance systems. http://www.its.dot.gov/cicas/ (Accessed on June 2011).
13. The NOW: Network on Wheels Project. Available at http://www.network-on-wheels.de (Accessed on June 2011).
14. U.S. Department of Transportation, Vehicle Safety Communications Project, 2006. Final Report, Public Document, Crash Avoidance Metrics Partnership.
15. H. Füßler, M. Transier, M. Torrent-Moreno, H. Hartenstein, and A. Festag. Thoughts on a protocol architecture for vehicular ad-hoc networks. In 2nd International Workshop on Intelligent Transportation (WIT 2005), Hamburg, Germany, 2005.
16. S. Yousefi and M. Fathy. Metrics for performance evaluation of safety applications in vehicular ad hoc networks. *Transport Vilnius: Technika*, vol. 23, no. 4, 2008, pp. 291–298.
17. J. Yin, T. ElBatt, G. Yeung, B. Ryu, S. Habermas, H. Krishnan, and T. Talty.Performance evaluation of safety applications over DSRC vehicular ad hoc networks. In *Proceedings of the 1st ACM International Workshop on Vehicular Ad Hoc Networks*, 2004, pp. 1–9.
18. T. Camp, J. Boleng, and V. Davies. A survey of mobility models for ad hoc network research. *Wireless Communications & Mobile Computing (WCMC)*, vol. 2, no. 5 (Special issue on Mobile Ad Hoc Networking: Research, Trends and Applications), 2002, pp. 483–502.
19. Quadstone Paramics, 2008. Available at http://www.paramicsonline.com (Accessed on June 2011).
20. *CORSIM User Manual*, Version 1.01. Washington, DC: U.S. Department Of Transportation, Federal Highway Administration, 1996.
21. D. Krajzewicz and C. Rossel. Simulation of urban mobility (SUMO). German Aerospace Centre, 2007. Available at http://sumo.sourceforge.net/index.shtml (Accessed on June 2011).
22. MOVE (MObility model generator for VEhicular networks): rapid generation of realistic simulation for VANET, 2007. Available at http://lens1.csie.ncku.edu.tw/MOVE/index.htm (Accessed on June 2011).
23. FreeSim, 2008. Available at http://www.freewaysimulator.com/ (Accessed on June 2011).
24. F.J. Martinez, J.C. Cano, C.T. Calafate, P. Manzoni. Citymob: a mobility model pattern generator for VANETs. In IEEE Vehicular Networks and Applications Workshop (Vehi-Mobi, held with ICC), Beijing, China, May 2008.
25. J. Haerri, M. Fiore, F. Fethi, and C. Bonnet. VanetMobiSim: generating realistic mobility patterns for VANETs. Institut Eurécom and Politecnico Di Torino, 2006. Available at http://vanet.eurecom.fr/ (Accessed on June 2011).

26. STRAW—STreet RAndom Waypoint—vehicular mobility model for network simulations (e.g., car networks), 2008. Available at http://www.aqualab.cs.northwestern.edu/projects/STRAW/index.php (Accessed on June 2011).
27. F.J. Martinez, C.K. Toh, J.C. Cano, C.T. Calafate, and P. Manzoni. A survey and comparative study of simulators for vehicular ad hoc networks (VANETs). *Wireless Communications and Mobile Computing*, 2009. Available at http://onlinelibrary.wiley.com/doi/10.1002/wcm.859/abstract (Accessed on June 2011).
28. OPNET Technologies, 2008. Available at http://www.opnet.com/ (Accessed on February 2011).
29. Scalable Network Technologies. QualNet. Scalable Network Technologies, Inc., 2006. Available at http://www.scalable-networks.com/products/qualnet/ (Accessed on June 2011).
30. The Network Simulator (ns-2). Available at http://www.isi.edu/nsnam/ns/ (Accessed on June 2011).
31. GloMoSim Network Simulator. Available at http://pcl.cs.ucla.edu/projects/glomosim/ (Accessed on June 2011).
32. OMNET++ Network Simulation Framework. Available at http://www.omnetpp.org (Accessed on June 2011).
33. JiST/SWANS: Java in Simulation Time/Scalable Wireless Ad hoc Network Simulator, 2004. Available at http://jist.ece.cornell.edu/ (Accessed on June 2011).
34. K. Walsh and E.G. Sirer. A staged network simulator (SNS). Computer Science Department, Cornell University, 2003. Available at http://www.cs.cornell.edu/people/egs/sns/ (Accessed on June 2011).
35. TraNS (Traffic and Network Simulation Environment). Available at http://trans.epfl.ch/ (Accessed on June 2011).
36. Veins (Vehicles in Network Simulation). Available at http://www7.informatik.uni-erlangen.de/~sommer/omnet/traci/ (Accessed on June 2011).
37. NCTUns 5.0, 2008. Available at http://nsl10.csie.nctu.edu.tw/ (Accessed on June 2011).
38. S. Schutz, L. Eggert, S. Schmid, and M. Brunner. Protocol enhancements for intermittently connected hosts. *ACM SIGCOMM Computer Communication Review*, vol. 35 no. 3, 2005, pp. 5–18.
39. T. Goff, J. Moronski, D.S. Phatak, and V. Gupta. Freeze-TCP: a true end-to-end TCP enhancement mechanism for mobile environments. In Proceedings of the 19th IEEE Conference on Computer Communications (INFOCOM), 2000.
40. A. Al Hanbali, E. Altman, and P. Nain. A survey of TCP over ad hoc networks. *IEEE Communications Surveys & Tutorials*, Vol. 7, no. 3, 2005, pp. 22–36.
41. M. Bechler, S. Jaap, and L. Wolf. An optimized TCP for Internet access of vehicular ad hoc networks. In *The Networking 2005*. LNCS No. 3462. Berlin: Springer, 2005.
42. S. Yousefi, T. Chahed, M. Moosavi, and K. Zayer. Comfort applications in vehicular ad hoc networks based on fountain coding. In IEEE WiVec 2010, Taipei, May 2010.
43. D.J. MacKay. *Information Theory, Inference, and Learning Algorithms*. Cambridge, UK: Cambridge University Press, 2003.
44. M.A. Shokrollahi. Raptor codes. In IEEE International Symposium on Information Theory, July 2003.
45. V. Bychkovsky, B. Hull, A. Miu, H. Balakrishnan, and S. Madden. A measurement study of vehicular Internet access using in situ Wi-Fi networks. In Proceedings of the 12th Annual International Conference on Mobile Computing and Networking (MobiCom 2006), 2006, pp. 50–61.
46. Y. Zhang, J. Zhao, and G. Cao. On scheduling vehicle-roadside data access.. In Proceedings of ACM VANET'07, in conjunction with Mobicom'07, Montreal, Canada, September 2007.
47. M. Shahverdy, M. Fathy, and S. Yousefi. Scheduling algorithm for vehicle to road-side data distribution. In *ICHCC-ICTMF 2009, China. Communications in Computer and Information Science* (CCIS Book Series), vol. 66. Berlin: Springer, 2010, pp. 30–38.
48. J. Mittag, F. Thomas, J. Härri, and H. Hartenstein. A comparison of single- and multi-hop beaconing in VANETs. In Proceedings of the Sixth ACM International Workshop on VehiculAr InterNETworking (VANET'09), 2009.
49. S. Yousefi, M. Fathy, and A. Benslimane. Performance of beacon safety message dissemination in Vehicular Ad hoc NETworks (VANETs). *Journal of Zhejiang University Science A*, vol. 8, no. 12, 2007, pp. 1990–2004.

50. M. TorrentMoreno, I. Mittag, P. Santi, and H. Hartenstein. Vehicle-to-vehicle .communication: fair transmit power control for safety-critical information. *IEEE Transactions on Vehicular Technology*, vol. 58, no. 7, 2009, pp. 3684–3703.
51. M. Armaghan, M. Fathy, and S. Yousefi. Improving the performance of beacon safety message dissemination in vehicular networks using Kalman filter estimation. In *FGCN 2009, Korea. Communications in Computer and Information Science* (CCIS Book Series), vol. 56. Berlin: Springer, 2009, pp. 74–82.
52. V. Sadatpour, M. Fathy, S. Yousefi, A.M. Rahmani, E.-S. Cho, and M.-K. Choi. Scheduling algorithm for beacon safety message dissemination in vehicular ad-hoc networks. In *FGCN 2009, Korea. Communications in Computer and Information Science* (CCIS Book Series), vol. 56. Berlin: Springer, 2009, pp. 133–140.
53. S. Rezaei, R. Sengupta, H. Krishnan, X. Guan, and R. Bhatia. Tracking the position of neighboring vehicles using wireless communications. *Transportation Research Part C: Emerging Technologies*, vol. 18, no. 3, 2010, pp. 335–350.
54. G. Welch and G. Bishop An introduction to the Kalman filter. Technical Report. UMI Order Number TR95-041, University of North Carolina at Chapel Hill, 1995.
55. W.R. Chang, H.T. Lin, and B.X. Chen. TrafficGather: an efficient and scalable data collection protocol for vehicular ad hoc networks. In Proceedings of the IEEE CCNC, 2008.
56. M.M. Artimy, W. Robertson, and W.J. Phillips. Connectivity with static transmission range in vehicular ad hoc networks. In *Proceedings of the 3rd Annual Communication Networks and Services Research Conference*, 2005, pp. 237–242.
57. M.M. Artimy, W. Robertson, and W.J. Phillips. Assignment of dynamic transmission range based on estimation of vehicle density. In *Proceedings of the 2nd ACM International Workshop on Vehicular Ad hoc Networks (VANET)*, 2005, pp. 40–48.
58. S. Yousefi, E. Altman, R. El-Azouzi, and M. Fathy. Analytical model for connectivity in vehicular ad hoc networks. *IEEE Transactions on Vehicular Technology*, vol. 57, no. 6, 2008, pp. 3341–3356.
59. N. Wisitpongphan, F. Bai, P. Mudalige, V. Sadekar, and O. Tonguz. Routing in sparse vehicular ad hoc wireless networks. *IEEE Journal on Selected Areas in Communications*, vol. 25, no. 8, 2007, pp. 1538–1556.
60. D. Miorandi and E. Altman. Connectivity in one-dimensional ad hoc networks: a queuing theoretical approach. *Wireless Networks*, vol. 12, no. 6, 2006, pp. 573–587.
61. M. Kijima and M. Ohnishi. Stochastic orders and their applications in financial optimization. *Mathematical Methods of Operations Research*, vol. 50, no. 2, 1999, pp. 351–372.
62. M. Rudack, M. Meincke, and M. Lott. On the dynamics of ad hoc networks for inter-vehicles communications (IVC). In *Proceedings of ICWN*, 2002, pp. 40–48.
63. S. Yousefi, E. Altman, R. El-Azouzi, and M. Fathy. Improving connectivity in vehicular ad hoc networks: an analytical study. *Computer Communications*, vol. 31, no. 9, 2008, pp. 1653–1659.
64. K.C. Lee, U. Lee, and M. Gerla. Survey of routing protocols in vehicular ad hoc networks. In Advances in Vehicular Ad-Hoc Networks: Developments and Challenges, IGI Global, October 2009.
65. A. Iwata. Scalable routing strategies for ad-hoc wireless networks. In *IEEE JSAC*, August 1999, pp. 1369–1379.
66. C.E. Perkins and E.M Royer. Ad-hoc on-demand distance vector routing. In *Proceedings of the IEEE WMCSA'99, New Orleans, LA*, February 1999, pp. 90–100.
67. V. Naumov, R. Baumann, and T. Gross. An evaluation of inter-vehicle ad hoc networks based on realistic vehicular traces. In Proceedings of the ACM MobiHoc'06 Conference, May 2006.
68. D.B. Johnson and D.A Maltz. Dynamic source routing in ad hoc wireless networks. In T. Imielinski and H. Korth (eds.), *Mobile Computing.* Massachusetts: Kluwer Academic Publishers, 1996, Ch. 5, pp. 153–181.
69. V. Namboodiri, M. Agarwal, and L. Gao. A study on the feasibility of mobile gateways for vehicular ad-hoc networks. In *Proceedings of the First International Workshop on Vehicular Ad Hoc Networks*, 2004, pp. 66–75.
70. C.-C. Ooi and N. Fisal. Implementation of geocast-enhanced AODV-bis routing protocol in MANET. In *Proceedings of the IEEE Region 10 Conference*, vol. 2, 2004, pp. 660–663.

71. Y.-B. Ko and N.H. Vaidya. Location-aided routing (LAR) in mobile ad hoc networks. *Wireless Networks*, vol. 6, no. 4, 2000, pp. 307–321.
72. L. Briesemeister, L. Schäfers, and G. Hommel. Disseminating messages among highly mobile hosts based on inter-vehicle communication. In *Proceedings of the IEEE Intelligent Vehicles Symposium*, 2000, pp. 522–527.
73. Y.-C. Hu, A. Perrig, and D.B. Johnson. ARIADNE: a secure on-demand routing protocol for ad hoc networks. In *Proceedings of ACM International Conference on Mobile Computing and Networking (MOBICOM'02), Atlanta, GA,* September 2002, pp. 12–23.
74. T. Yu, G.H. Lu, and Z.L. Zhang. Enhancing location service scalability with high grade. In IEEE International Conference on Mobile Ad-hoc and Sensor Systems, October 25–27, 2004, pp. 164–173.
75. J. Zhao and G. Cao. VADD: vehicle-assisted data delivery in vehicular ad hoc networks. In *Proceedings of 25th IEEE International Conference on Computer Communications*, April 2006, pp. 1–12.
76. B. Karp and H.T. Kung. GPSR: greedy perimeter stateless routing for wireless networks. In *Proceedings of Mobile Computing and Networking*, 2000, pp. 243–254.
77. I. Leontiadis and C. Mascolo. GeOpps: geographical opportunistic routing for vehicular networks. In *IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, June 18–21, 2007, pp. 1–6.
78. G. Toussaint. The relative neighborhood graph of a finite planar set. *Pattern Recognition*, vol. 12, no. 12, 1980, pp. 231–268.
79. K.R. Gabriel and R. Sokal. A new statistical approach to geographic variation analysis. *Systematic Zoology*, vol. 18, 1969, pp. 231–268.
80. S. Schnaufer, H. Füßler, M. Transier, and W. Effelsberg. Unicast ad-hoc routing in vehicular city scenarios. TR-2007-012, University of Mannheim, Mannheim, Germany.
81. S. Schnaufer and W. Effelsberg. Position-based unicast routing for city scenarios. In *International Symposium on a World of Wireless, Mobile and Multimedia Networks*, June 23–26, 2008, pp. 1–8.
82. C. Lochert, M. Mauve, H. F¨ussler, and H. Hartenstein. Geographic routing in city scenarios. *SIGMOBILE Mobile Computing and Communications Review*, vol. 9, no. 1, 2005, pp. 69–72.
83. C. Lochert, H. Hartenstein, J. Tian, H. Fussler, D. Hermann, and M. Mauve. A routing strategy for vehicular ad hoc networks in city environments. In *Proceedings of IEEE Intelligent Vehicles Symposium*, June 9–11, 2003, pp. 156–161.
84. B.C. Seet, G. Liu, B.S. Lee, C.H. Foh, K.J. Wong, and K.K. Lee. A-STAR: a mobile ad hoc routing strategy for metropolis vehicular communications. In *Proceedings of the 3rd International IFIP-TC6 Networking Conference*, Athens, Greece, Lecture Notes in computer Science (LNCS), May 9–14, 2004, pp. 989–999.
85. D. Forderer. Street-topology based routing. Master's thesis, University of Mannheim, May 2005.
86. M. Jerbi, S.M. Senouci, R. Meraihi, and Y. Ghamri-Doudane. An improved vehicular ad hoc routing protocol for city environments. In *IEEE International Conference on Communications, 2007 (ICC'07)*, June 24–28, 2007, pp. 3972–3979.
87. K. Lee, M. Le, J. Haerri, and M. Gerla. Louvre: landmark overlays for urban vehicular routing environments. In Proceedings of IEEE WiVeC, 2008.
88. H. Füßler, H. Hannes, W. Jorg, M. Martin, and E. Wolfgang. Contention-based forwarding for street scenarios. In *Proceedings of the 1st International Workshop in Intelligent Transportation (WIT 2004), Hamburg, Germany*, March 2004, pages 155–160.
89. Y. Shao, C. Liu, and J. Wu. Delay tolerant networks in VANETs. In *Vehicular Networks: From Theory to Practice*, S. Olariu and M. C. Weigle (Eds.) Chapman and Hall/CRC, 2009.
90. A. Bachir and A. Benslimane. A multicast protocol in ad hoc networks inter-vehicle geocast. In Proceedings of IEEE VTC, 2003.
91. M. Torrent-Moreno, D. Jiang, and H. Hartenstein. Broadcast reception rates and effects of priority access in 802.11-based vehicular ad-hoc networks. In Proceedings of ACM VANET, 2004.
92. G. Korkmaz, E. Ekici, F. Ozguner, and U. Ozguner. Urban multi-hop broadcast protocol for inter-vehicle communication systems. In Proceedings of ACM VANET, October 2004.

93. N. Wisitpongphan, O.K. Tonguz, J.S. Parikh, P. Mudalige, F. Bai, and V. Sadekar. Broadcast storm mitigation techniques in vehicular ad hoc networks. *IEEE Wireless Communication*, vol. 14, 2007, pp. 84–89.
94. G. Korkmaz, E. Ekici, and F. Ozguner. An efficient fully ad-hoc multi-hop broadcast protocol for inter-vehicular communication systems. In Proceedings of IEEE ICC, 2006.
95. Z. Haas, J.Y. Halpern, and L. Li. Gossip-based ad hoc routing. In Proceedings of IEEE INFOCOM, 2002.
96. A. Vahdat and D. Becker. Epidemic routing for partially connected ad hoc networks, Technical Report (CS-2000-06), Department of Computer Science, Duke University, Durham, NC, April 2000.
97. T. Spyropoulos, K. Psounis, and C.S. Raghavendra. Spray and wait: an efficient routing scheme for intermittently connected mobile networks. In Proceedings of ACM SIGCOMM Workshop on Delay-Tolerant Networking, 2005.
98. A. Lindgren, A. Doria, and O. SchelSn. Probabilistic routing in intermittently connected networks. In Poster of ACM MOBIHOC, 2003.
99. J. Leguay, T. Friedman, and V. Conan. Evaluating mobility pattern space routing for DTNs. In Proceedings of IEEE INFOCOM, 2006.
100. IEEE 802.16-2004. Local and metropolitan networks—Part 16: air interface for fixed broadband wireless access systems, 2004.
101. IEEE 802.16e-2005. Local and metropolitan networks—Part 16: air interface for fixed and mobile broadband wireless access systems, amendment 2: physical and medium access control layers for combined fixed and mobile operation in licensed bands and corrigendum 1, 2006.
102. A. Costa, P. Pedreiras, J. Fonseca, H. Proença, Á. Gomes, and J.S. Gomes. Evaluating WiMAX for vehicular communication applications. In IEEE International Conference on Emerging Technologies and Factory Automation (ETFA 2008), 2008.
103. Y. Ge, S. Wen, Y.-H. Ang, and Y.-C. Liang. Optimal relay selection in IEEE 802.16j multihop relay vehicular networks. *IEEE Transactions on Vehicular Technology*, vol. 59, no. 5, 2010, pp. 2198–2206.
104. J. Mar, S.E. Chen, and Y.R. Lin. The effect of the MS speed on the traffic performance of an integrated mobile WiMAX and DSRC multimedia networks on the highway. In *Proceedings of the ACM IWCMC*, August 2007, pp. 43–48.
105. T. Tsuboi, J. Yamada, N. Yamauchi, and N. Yoshikawa. WAVE design for next DSRC applications. In IEEE Proceedings of the 9th Conference on Wireless Telecommunications Symposium, 2010.
106. S. Yousefi, M.S. Mousavi, and M. Fathy. Vehicular ad hoc networks (VANETs): challenges and perspectives. In *Proceedings of the 6th IEEE International Conference ITST, Chengdu, China*, 2006, pp. 761–766.