Telecommun Syst
DOI 10.1007/s11235-010-9400-5

Vehicular ad hoc networks (VANETS): status, results, and challenges

Sherali Zeadally · Ray Hunt · Yuh-Shyan Chen · Angela Irwin · Aamir Hassan

Abstract Recent advances in hardware, software, and communication technologies are enabling the design and implementation of a whole range of different types of networks that are being deployed in various environments. One such network that has received a lot of interest in the last couple of years is the Vehicular Ad-Hoc Network (VANET). VANET has become an active area of research, standardization, and development because it has tremendous potential to improve vehicle and road safety, traffic efficiency, and convenience as well as comfort to both drivers and passengers. Recent research efforts have placed a strong emphasis on novel VANET design architectures and implementations. A lot of VANET research work have focused on specific areas including routing, broadcasting, Quality of Service (QoS), and security. We survey some of the recent research results in these areas. We present a review of wireless access standards for VANETs, and describe some of the recent VANET trials and deployments in the US, Japan, and the European Union. In addition, we also briefly present some of the simulators currently available to VANET researchers for VANET simulations and we assess their benefits and limitations. Finally, we outline some of the VANET research challenges that still need to be addressed to enable the ubiquitous deployment and widespead adoption of scalable, reliable, robust, and secure VANET architectures, protocols, technologies, and services.

Keywords Networking · VANET · Protocols · Standards · Routing · Security · Broadcasting · Simulation

S. Zeadally (✉)
Network Systems Laboratory, Department of Computer Science and Information Technology, University of the District of Columbia, 4200, Connecticut Avenue, N.W., Washington, DC 20008, USA
e-mail: szeadally@udc.edu

R. Hunt
Department of Computer Science and Software Engineering, College of Engineering, University of Canterbury, Private Bag 4800, Christchurch, New Zealand
e-mail: ray.hunt@canterbury.ac.nz

Y.-S. Chen
Department of Computer Science and Information Engineering, National Taipei University, 151, University Rd., San Shia, Taipei County, Taiwan
e-mail: yschen@mail.ntpu.edu.tw

Y.-S. Chen
e-mail: yschen@csie.ntpu.edu.tw

Y.-S. Chen
e-mail: yschen.iet@gmail.com

A. Irwin
School of Computer and Information Science, University of South Australia, Room F2-22a, Mawson Lakes, South Australia 5095, Australia
e-mail: angela.irwin@unisa.edu.au

A. Hassan
School of Information Science, Computer and Electrical Engineering, Halmstad University, Kristian IV:s väg 3, 301 18 Halmstad, Sweden
e-mail: aamhas06@student.hh.se

1 Introduction

Vehicular Ad Hoc Networks (VANETs) have grown out of the need to support the growing number of wireless products that can now be used in vehicles [1, 2]. These products include remote keyless entry devices, personal digital assistants (PDAs), laptops and mobile telephones. As mobile wireless devices and networks become increasingly important, the demand for Vehicle-to-Vehicle (V2V) and Vehicle-

to-Roadside (VRC) or Vehicle-to-Infrastructure (V2I) Communication will continue to grow [2]. VANETs can be utilized for a broad range of safety and non-safety applications, allow for value added services such as vehicle safety, automated toll payment, traffic management, enhanced navigation, location-based services such as finding the closest fuel station, restaurant or travel lodge [3] and infotainment applications such as providing access to the Internet.

Over the last few years, we have witnessed many research efforts that have investigated various issues related to V2I, V2V, and VRC areas because of the crucial role they are expected to play in Intelligent Transportation Systems (ITSs). In fact, various VANET projects have been executed by various governments, industries, and academic institutions around the world in the last decade or so.

The rest of the paper is organized as follows. Section 2 presents an overview of VANET. In Sect. 3, we present wireless access standards that are being deployed for VANETs. Section 4 discusses some of the latest VANET research results on security, routing, Quality of Service, and broadcasting. In Sect. 5, we present some of recent VANET projects undertaken by various groups and organizations in the US, Japan, and the European Union. Section 6 presents an evaluation of VANET simulators and highlights their benefits and limitations. Some of the VANET research challenges that still require innovative solutions are presented in Sect. 7. Finally, we make some concluding remarks in Sect. 8.

2 Overview of VANET

2.1 Intelligent transportation systems (ITSs)

In intelligent transportation systems, each vehicle takes on the role of sender, receiver, and router [4] to broadcast information to the vehicular network or transportation agency, which then uses the information to ensure safe, free-flow of traffic. For communication to occur between vehicles and RoadSide Units (RSUs), vehicles must be equipped with some sort of radio interface or OnBoard Unit (OBU) that enables short-range wireless ad hoc networks to be formed [5]. Vehicles must also be fitted with hardware that permits detailed position information such as Global Positioning System (GPS) or a Differential Global Positioning System (DGPS) receiver. Fixed RSUs, which are connected to the backbone network, must be in place to facilitate communication. The number and distribution of roadside units is dependent on the communication protocol is to be used. For example, some protocols require roadside units to be distributed evenly throughout the whole road network, some require roadside units only at intersections, while others require roadside units only at region borders. Though it is safe to assume that infrastructure exists to some extent and vehicles have access to it intermittently, it is unrealistic to require that vehicles always have wireless access to roadside units. Figures 1, 2 and 3 depict the possible communication configurations in intelligent transportation systems. These include inter-vehicle, vehicle-to-roadside, and routing-based communications. Inter-vehicle, vehicle-to-roadside, and routing-based communications rely on very accurate and up-to-date information about the surrounding environment, which, in turn, requires the use of accurate positioning systems and smart communication protocols for exchanging information. In a network environment in which the communication medium is shared, highly unreliable, and with limited bandwidth [6], smart communication protocols must guarantee fast and reliable delivery of information to all vehicles in the vicinity. It is worth mentioning that Intra-vehicle communication uses technologies such as IEEE 802.15.1 (Bluetooth), IEEE 802.15.3 (Ultra-wide Band) and IEEE 802.15.4 (Zigbee) that can be used to support wireless communication inside a vehicle but this is outside the scope of this paper and will not be discussed further.

2.1.1 *Inter-vehicle communication*

The inter-vehicle communication configuration (Fig. 1) uses multi-hop multicast/broadcast to transmit traffic related information over multiple hops to a group of receivers.

In intelligent transportation systems, vehicles need only be concerned with activity on the road ahead and not behind (an example of this would be for emergency message dissemination about an imminent collision or dynamic route scheduling). There are two types of message forwarding in inter-vehicle communications: *naïve broadcasting* and *intelligent broadcasting*. In *naïve broadcasting*, vehicles send broadcast messages periodically and at regular intervals. Upon receipt of the message, the vehicle ignores the message if it has come from a vehicle behind it. If the message comes from a vehicle in front, the receiving vehicle sends its own broadcast message to vehicles behind it. This ensures that all enabled vehicles moving in the forward direction get all broadcast messages. The limitations of the naïve

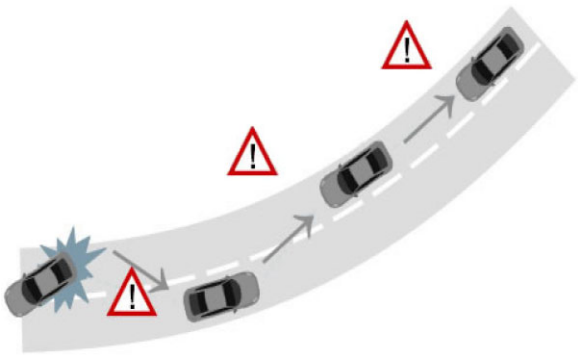

Fig. 1 Inter-vehicle communication

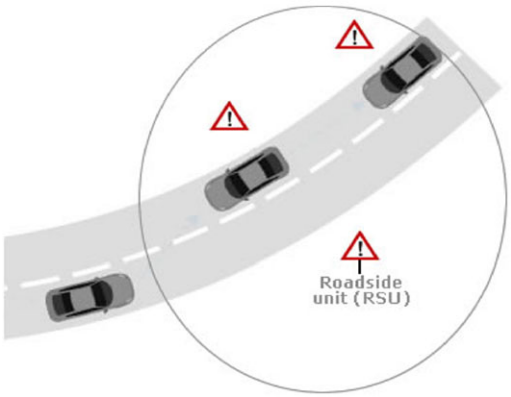

Fig. 2 Vehicle-to-roadside communication

broadcasting method is that large numbers of broadcast messages are generated, therefore, increasing the risk of message collision resulting in lower message delivery rates and increased delivery times [7]. *Intelligent broadcasting* with implicit acknowledgement addresses the problems inherent in naïve broadcasting by limiting the number of messages broadcast for a given emergency event. If the event-detecting vehicle receives the same message from behind, it assumes that at least one vehicle in the back has received it and ceases broadcasting. The assumption is that the vehicle in the back will be responsible for moving the message along to the rest of the vehicles. If a vehicle receives a message from more than one source it will act on the first message only.

2.1.2 Vehicle-to-roadside communication

The vehicle-to-roadside communication configuration (Fig. 2) represents a single hop broadcast where the roadside unit sends a broadcast message to all equipped vehicles in the vicinity.

Vehicle-to-roadside communication configuration provides a high bandwidth link between vehicles and roadside units. The roadside units may be placed every kilometer or less, enabling high data rates to be maintained in heavy traffic. For instance, when broadcasting dynamic speed limits, the roadside unit will determine the appropriate speed limit according to its internal timetable and traffic conditions. The roadside unit will periodically broadcast a message containing the speed limit and will compare any geographic or directional limits with vehicle data to determine if a speed limit warning applies to any of the vehicles in the vicinity. If a vehicle violates the desired speed limit, a broadcast will be delivered to the vehicle in the form of an auditory or visual warning, requesting that the driver reduce his speed.

2.1.3 Routing-based communication

The routing-based communication configuration (Fig. 3) is a multi-hop unicast where a message is propagated in a multi-hop fashion until the vehicle carrying the desired data is reached.

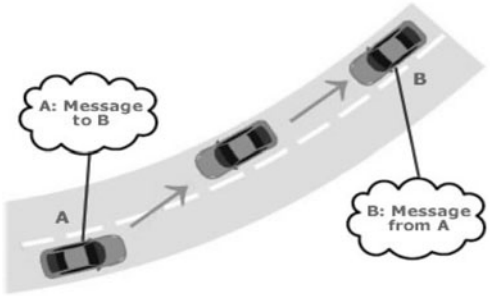

Fig. 3 Routing-based communication

When the query is received by a vehicle owning the desired piece of information, the application at that vehicle immediately sends a unicast message containing the information to the vehicle it received the request from, which is then charged with the task of forwarding it towards the query source.

3 Standards for wireless access in VANETs

Standards simplify product development, help reduce costs, and enable users to compare competing products. Only through the use of standards can the requirements of interconnectivity and interoperability be guaranteed and the emergence of new products be verified to enable the rapid implementation of new technologies. There are many standards that relate to wireless access in vehicular environments. These standards range from protocols that apply to transponder equipment and communication protocols through to security specification, routing, addressing services, and interoperability protocols.

3.1 Dedicated Short Range Communication (DSRC)

Dedicated Short Range Communications (DSRC) is a short to medium range communications service that was developed to support vehicle-to-vehicle and vehicle-to-roadside communications. Such communications cover a wide range of applications, including vehicle-to-vehicle safety messages, traffic information, toll collection, drive-through payment, and several others. DSRC is aimed at providing high data transfers and low communication latency in small communication zones. In 1999, the United States Federal Communications Commission (FCC) allocated 75 MHz of spectrum at 5.9 MHz to be used by DSRC. In 2003, The American Society for Testing and Materials (ASTM)[1] approved

[1] ASTM is a voluntary standards development organization for technical standards for material products, systems, and services.

Table 1 DSRC standards in Japan, Europe, and the US

Features	JAPAN (ARIB)	EUROPE (CEN)	USA (ASTM)
Communication	Half-duplex (OBU)/Full duplex (RSU)	Half-duplex	Half-duplex
Radio Frequency	5.8 GHz band	5.8 GHz band	5.9 GHz band
Band	80 MHz bandwidth	20 MHz bandwidth	75 MHz bandwidth
Channels	Downlink: 7	4	7
	Uplink: 7		
Channel Separation	5 MHz	5 MHz	10 MHz
Data Transmission rate	Down/Up-link	Down-link/500 Kbits/s	Down/Up-link
	1 or 4 MBits/s	Up-link/ 250 Kbits/s	3-27 Mbits/s
Coverage	30 meters	15–20 meters	1000 meters (max)
Modulation	2-ASK, 4-PSK	RSU: 2-ASK	OFDM
		OBU: 2-PSK	

ARIB: Association of Radio Industries and Businesses
CEN: European Committee for Standardization
ASTM: American Society for Testing and Materials
OBU: On-Board Unit
RSU: Road Side Unit
ASK: Amplitude Shift Keying
PSK: Phase Shift Keying
OFDM: Orthogonal Frequency Division Multiplexing

the ASTM-DSRC standard which was based on the IEEE 802.11a physical layer and 802.11 MAC layer [8]. This standard was later published as ASTM E2213-03. In February 2004, the report issued by the FCC established service and licensing rules that govern the use of the DSRC band. DSRC is a free but licensed spectrum. It is free since the FCC does not charge for usage of that spectrum but it is licensed which means that it is more restricted in terms of its usage [9]. For instance, the FCC requires the use of specific channels and all radios developed should conform to the standard. The DSRC spectrum is organized into 7 channels each of which is 10 MHz wide. One channel is restricted for safety communications only while two other channels are reserved for special purposes (such as critical safety of life and high power public safety). All the remaining channels are service channels which can be used for either safety or non-safety applications. Safety applications are given higher priority over non-safety applications to avoid their possible performance degradations and at the same time save lives by warning drivers of imminent dangers or events to enable timely corrective actions to be taken. We compare recent regional standards for DSRC in Table 1 [10]. For a more in-depth discussion of DSRC, the reader is referred to [8, 11].

3.2 IEEE 1609—standards for wireless access in vehicular environments (WAVE) (IEEE 802.11p)

Wireless connectivity between moving vehicles can be provided by existing 802.11a compliant devices with data rates of up to 54 Mbps being achieved with 802.11a hardware [14]. However, vehicular traffic scenarios have greater challenges than fixed wireless networks, caused by varying driving speeds, traffic patterns, and driving environments. Traditional IEEE 802.11 Media Access Control (MAC) operations suffer from significant overheads when used in vehicular scenarios. For instance, to ensure timely vehicular safety communications, fast data exchanges are required. In these circumstances the scanning of channels for beacons from an Access Point along with multiple handshakes required to establish communication are associated with too much complexity and high overheads (for example, in the case of a vehicle encountering another vehicle coming in the opposite direction, the duration for possible communication between them is extremely short [12] making it difficult to establish communications). To address these challenging requirements of IEEE MAC operations, the DSRC effort of the ASTM 2313 working group migrated to the IEEE 802.11 standard group which renamed the DSRC to IEEE 802.11p Wireless Access in Vehicular Environments (WAVE) [15].

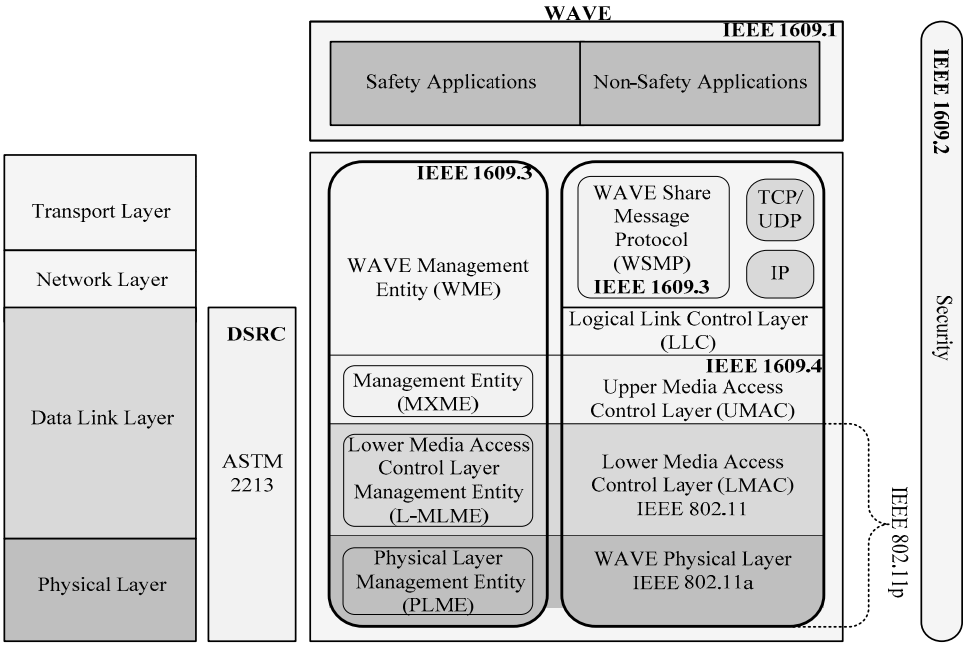

Fig. 4 Wireless access in vehicular environments (WAVE), IEEE 1609, IEEE 802.11p and the OSI reference model

ASTM: American Society for Testing and Materials
DSRC: Dedicated Short Range Communication
IP: Internet Protocol
TCP: Transmission Control Protocol
UDP: User Datagram Protocol

In contrast to the regional standards of DSRC, by incorporating DSRC into IEEE 802.11, WAVE will become a standard that can be universally adopted across the world. As illustrated in Fig. 4, it is worth noting that IEEE 802.11p is limited by the scope of IEEE 802.11 which strictly works at the media access control and physical layers [13]. The operational functions and complexity related to DSRC are handled by the upper layers of the IEEE 1609 standards. These standards define how applications that utilize WAVE will function in the WAVE environment, based on the management activities defined in IEEE P1609.1, the security protocols defined in IEEE P1609.2, and the network-layer protocol defined in IEEE P1609.3. The IEEE 1609.4 resides above 802.11p and this standard supports the operation of higher layers without the need to deal with the physical channel access parameters.

WAVE defines two types of devices: RoadSide Unit (RSU), and OnBoard Unit (OBU) which are essentially stationary and mobile devices respectively. RSUs and OBUs can be either a provider or a user of services and can switch between such modes. Normally stationary WAVE devices host an application that provides a service, and the mobile device which hosts a peer application that uses such a service. There may also be applications on devices remote from the RSU whose purpose is to provide services to the OBU. This WAVE standard describes applications that resides on the RSU but is designed to multiplex requests from remote applications thus providing them with access to the OBU. WAVE uses Orthogonal Frequency Division Multiplexing (OFDM) to split the signal into several narrowband channels to provide a data payload communication capability of 3, 4.5, 6, 9, 12, 18, 24 and 27 Mbps in 10 MHz channels.

A brief summary of the IEEE 1609/802.16e standards is given in Table 2.

4 Routing, QoS, broadcasting, and security in VANET

VANET has been an active field of research and development for years but it is fair to say that, with the recent dramatic improvements in communication and computing technologies, it is only in the last decade that this field has really gained a lot of momentum. In fact, VANET research has attracted a lot of attention from researchers working in various fields including electronics, networking, security, software engineering, automotive, transportation, and so on. Recent results covering VANET-related issues include areas such as routing, Quality Service (QoS), broadcasting, security attacks and threats, capacity, collision and interference, the effects of transmission power on protocol performance and power control algorithms, congestion control, and service discovery. It is beyond the scope of this work to review each of these topics. Instead, we present, discuss, and review recent research results that have been achieved in the most active VANET areas which include routing, broadcasting, QoS, and security. In addition, the rationale for selecting

Table 2 IEEE 1609/802.16e standards

IEEE Standard	Reference	Description
IEEE Standard 1609	[16]	Defines the overall architecture, communication model, management structure, security mechanisms and physical access for wireless communications in the vehicular environment, the basic architectural components such as OBU, RSU, and the WAVE interface.
IEEE Standard 1609.1-2006	[17]	Enables interoperability of WAVE applications, describes major components of the WAVE architecture, and defines command and storage message formats.
IEEE Standard 1609.2-2006	[18]	Describes security services for WAVE management and application messages to prevent attacks such as eavesdropping, spoofing, alteration, and replay.
IEEE Standard 1609.3-2007	[19]	Specifies addressing and routing services within a WAVE system to enable secure data exchange, enables multiple stacks of upper/lower layers above/below WAVE networking services, defines WAVE Short Message Protocol (WSMP) as an alternative to IP for WAVE applications.
IEEE Standard 1609.4-2006	[20]	Describes enhancements made to the 802.11 Media Access Control Layer to support WAVE.
IEEE Standard 802.16e	[21]	Enables interoperable multi-vendor broadband wireless access products.

these specific areas also stems from the fact that they are the ones with the most active interest from the VANET research community as evidenced by the number of recent publications we found during our literature review on VANET.

4.1 Routing

Routing in VANET has been studied and investigated widely in the past few years [22–25]. Since VANETs are a specific class of ad hoc networks, the commonly used ad hoc routing protocols initially implemented for MANETs have been tested and evaluated for use in a VANET environment. Use of these address-based and topology-based routing protocols requires that each of the participating nodes be assigned a unique address. This implies that we need a mechanism that can be used to assign unique addresses to vehicles but these protocols do not guarantee the avoidance of allocation of duplicate addresses in the network [26]. Thus, existing distributed addressing algorithms used in mobile ad-hoc networks are much less suitable in a VANET environment. Specific VANET-related issues such as network topology, mobility patterns, demographics, density of vehicles at different times of the day, rapid changes in vehicles arriving and leaving the VANET and the fact that the width of the road is often smaller than the transmission range all make the use of these conventional ad hoc routing protocols inadequate.

4.1.1 Proactive routing protocols

Proactive routing protocols employ standard distance-vector routing strategies (e.g., Destination-Sequenced Distance-Vector (DSDV) routing) or link-state routing strategies (e.g., Optimized Link State Routing protocol (OLSR) and Topology Broadcast-based on Reverse-Path Forwarding (TBRPF)). They maintain and update information on routing among all nodes of a given network at all times even if the paths are not currently being used. Route updates are periodically performed regardless of network load, bandwidth constraints, and network size. The main drawback of such approaches is that the maintenance of unused paths may occupy a significant part of the available bandwidth if the topology of the network changes frequently. Since a network between cars is extremely dynamic proactive routing algorithms are often inefficient.

4.1.2 Reactive routing protocols

Reactive routing protocols such as Dynamic Source Routing (DSR), and Ad hoc On-demand Distance Vector (AODV) routing implement route determination on a demand or need basis and maintain only the routes that are currently in use, thereby reducing the burden on the network when only a subset of available routes is in use at any time. Communication among vehicles will only use a very limited number of routes, and therefore reactive routing is particularly suitable for this application scenario.

4.1.3 Position-based routing

Position-based routing protocols [27] require that information about the physical position of the participating nodes be available. This position is made available to the direct neighbors in the form of periodically transmitted beacons. A sender can request the position of a receiver by means of a location service. The routing decision at each node is then based on the destination's position contained in the packet and the position of the forwarding node's neighbors. Consequently, position-based routing does not require the establishment or maintenance of routes. Examples of position-based routing algorithms include Greedy Perimeter Stateless

Routing (GPSR) [28] and Distance Routing Effect Algorithm for Mobility (DREAM) [29]. Karp et al. [28] describe a position-based routing protocol based on a greedy forwarding mechanism in which packets are forwarded through nodes geographically closer to the destination than the previous node. Thus the position of the next hop will always be closer to the destination node than that of the current hop. The "perimeter routing" mode of GPSR (greedy perimeter stateless routing) that searches for alternate routes that may not be geographically closer is not considered since in a highway scenario the width of the road is often smaller than the range of transmission. Thus in this scenario there is no way for a route to move away from the destination and still find its way back.

Existing ad hoc networks employ topology-based routing where routes are established over a fixed succession of nodes but which can lead to broken routes and a high overhead to repair these routes. The special conditions and requirements for vehicular communications, including frequent topology changes, short connectivity time and positioning systems have justified the development of dedicated routing solutions for wireless multi-hop communication based on geographic positions. The use of Global Positioning System (GPS) technology enables forwarding to be decoupled from a node's identity and therefore the position of the destination node is used rather than a route to it which requires traffic flow via a set of neighbors [2]. Thus position-based routing provides a more scalable and efficient forwarding mechanism appropriate for highly volatile ad hoc networks found in VANETs. Position based routing constitutes three core components: beaconing, location service and forwarding (geographic unicast and geographic broadcast): Four recent important initiatives in position-based routing include: Naumov et al. [30] describe a recent innovation protocol called Connectivity Aware Routing (CAR) for VANETs. It is a position based routing scheme capable of finding connected paths between source and destination pairs. Leontiadis et al. [31] describe a geographical opportunistic routing protocol suitable for vehicular networks which exploits the topology of VANETs as well as geographical routing information.

Hartenstein [32] describes a position-based routing scheme which employs a unique identifier such as an IP address which is used to identify a vehicle along with its current position (GPS coordinate). This scheme only requires that a vehicle knows its own position and that of its one-hop neighbours. Assuming a packet contains the destination position, the router forwards the packet to a node closer to the destination than itself. Given the relatively high speeds of the large number of vehicles involved, this scheme is both adaptive and scalable with respect to network topology.

4.1.4 Beaconing and location service

Vehicles periodically broadcast short packets with their identifier and current geographic position. Upon receipt of a beacon, a vehicle stores the information in its location table. The requesting vehicle issues a location query message requesting the identification and sequence numbers and hop limit when it needs to know the position of a required vehicle not available in its location table. This message is rebroadcast to nearby vehicles until it reaches the required vehicle or the hop limit is reached. If the request is not a duplicate, the required vehicle answers with a location reply message carrying its current position and timestamp. Upon receipt of the location reply, the originating vehicle updates its location table.

4.1.5 Forwarding

A geographic unicast transports packets between two nodes via multiple wireless hops. When the requesting node wishes to send a unicast packet, it determines the position of the destination node by looking at the location table. A greedy forwarding algorithm is then used to send the packet to the neighboring vehicle (see Fig. 5), detailing the minimum remaining distance to the destination vehicle and this process repeats at every vehicle along the forwarding path until the packet reaches its destination.

A geographic broadcast distributes data packets by flooding, where vehicles re-broadcast the packets if they are located in the geographic area determined by the packet. The application of advanced broadcasting algorithms help to minimize overhead by reducing the occurrence of broadcast storms. Data and control packet forwarding must be loop-free and towards the destination or target area location. Having packets forwarded across the shortest path towards the destination is not a requirement due to the high network volatility [2].

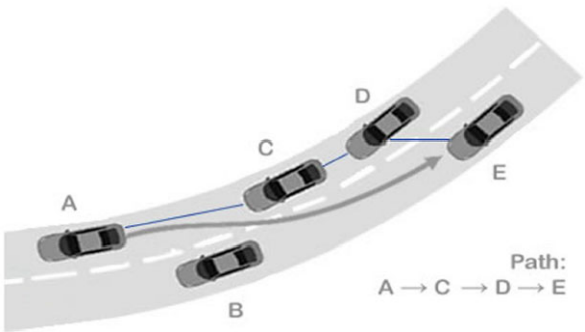

Fig. 5 Cached Greedy Geographic Unicast (CGGC) Example of a greedy unicast transmission based on knowledge of the destination's position

4.1.6 *Protocols for dedicated short-range communication (DSRC)*

Recent research on dedicated short-range communication protocols, namely Coordinated External Peer Communication (CEPEC) [34] and Communications Architecture for Reliable Adaptive Vehicular Ad Hoc Networks (CARAVAN) [33] use mapping and timeslot allocation to reduce the occurrence of denial of service attacks or attacks that burden the limited bandwidth available in vehicular networks.

Communications in a vehicular network are susceptible to denial of service attacks by jamming the communication medium or taxing the limited wireless bandwidth that is available. These attacks are possible due to the DSRC standard specification that a vehicle must wait to transmit until it senses that the channel is idle, allowing a malicious vehicle to constantly transmit noise to prevent transmission from within sensing range of the attacker vehicle. Blum & Eskandarian [33] present the Communications Architecture for Reliable Adaptive Vehicular Ad Hoc Networks (CARAVAN) as a solution to these types of communication attacks. CARAVAN uses Trusted Computing Platforms, spread spectrum technology and a secret pseudorandom spreading code to verify the integrity of the software and hardware of the sending vehicle before allowing the vehicle to transmit messages. CARAVAN includes a new link layer protocol called Adaptive Space Division Multiplexing (ASDM) that allocates timeslots to vehicles to maximize anti-jamming protection. ASDM includes original features that improve on existing Space Division Multiple Access (SDMA) protocols in terms of bandwidth utilization by splitting the roadway into discrete cells that can contain at most one vehicle. A mapping function is then defined that assigns each of the cells a timeslot. No two cells within a predefined range of each other will have the same timeslot. In their approach the physical layer is split into two frequency bands with radio ranges that are selected based on the requirements of the messages carried in each band. Irregularly occurring warning messages place a premium on network connectivity since they are of interest to vehicles far from the message source. These messages are relatively infrequent and therefore require less bandwidth. Periodic messages, on the other hand, are only of interest to vehicles close to the message source, but there are a large number of these messages and they must be generated frequently. The network protocol includes message forwarding rules and a method that leverages the benefits of varying radio ranges to speed delivery of irregular messages. The results of simulation studies demonstrate that with these new features, CARAVAN produces message propagation latencies that are similar to or better than less secure, currently proposed inter-vehicle communication protocols.

Yang et al. [34] propose a cross-layer protocol called Coordinated External Peer Communication (CEPEC) for peer-to-peer communications in vehicular networks. The CEPEC protocol coordinates the functions of physical, MAC and network layers to provide a fair and handoff-free solution for uplink packet delivery from vehicles to roadside unit. With CEPEC, the road is logically partitioned into segments of equal length and a relaying head is selected in each segment to perform local packet collecting and aggregate packet relaying. Nodes outside the coverage area of the nearest roadside unit can still get access via a multi-hop route to their roadside unit. Similar to CARAVAN, CEPEC allocates timeslots to vehicles in two steps: first, the roadside unit allocates the timeslots to the segments. Second, intra-segment timeslot allocation occurs where the Segment Head (SH) assigns timeslots to individual vehicles within the segment. Results show that the CEPEC protocol provides higher throughput with guaranteed fairness in multi-hop data delivery in VANETs when compared with a purely IEEE 802.16-based protocol.

4.2 Broadcasting

A geographic broadcast distributes data packets by flooding, where vehicles re-broadcast the packets if they are located in the geographic area determined by the packet. The application of broadcasting algorithms help to minimize overhead by reducing the occurrence of broadcast storms and is further addressed later in this section. Data and control packet forwarding must be loop-free and in the direction of the destination or target area location. Having packets forwarded across the shortest path towards the destination—typically found in conventional routing networks—is not a requirement due to the high network volatility [2].

As mentioned earlier, several past routing efforts have investigated the design of ad hoc routing algorithms suitable for operation in a VANET environment to deal with: a node's mobility, by discovering new routes (reactive routing algorithms), updating existing routing tables (proactive routing algorithms), using geographical location information (position-based routing algorithms), detecting stable vehicle configurations (clusters), using a vehicle's movements to support message transportation and using broadcasting to support message forwarding.

As stated earlier, vehicles periodically broadcast short packets with their identifiers and current geographic position. Upon receipt of such beacons, a vehicle stores the information in its location table. It is therefore possible to design a Cooperative Collision Avoidance (CCA) system that can assist in collision avoidance by delivering warning messages. When an emergency situation arises, a vehicle that is part of a CCA platoon needs to broadcast a message to all of the vehicles behind it. The vehicles that receive this message

selectively forward it based upon the direction from which it came which ensures that all members of the platoon eventually receive this warning.

Biswas et al. [35] discuss different types of forwarding, including naive and intelligent broadcasting. Naive broadcast forwarding requires the vehicle to send a broadcast message periodically at regular intervals. The receiving vehicle ignores this message if it comes from behind with respect to its direction of movement. If it comes from the front, it believes there must be an emergency in front and sends out periodic broadcast messages of its own. Thus, other vehicles in the platoon will eventually receive this warning message which will result in evasive action. A limitation of this approach results from the volume of forwarded messages. A result of this is that the number of 802.11 MAC message collisions can increase which in turn lowers the message delivery rate and increases the delivery time. This happens if the message is dropped and forces the event-detecting vehicle to periodically retransmit it. Biswas et al. [35] describes an intelligent broadcast protocol with implicit acknowledgement to address this problem. This protocol improves system performance by limiting the number of messages broadcast within the platoon for a given emergency. If the event-detecting vehicle receives the same message from behind, it assumes that at least one vehicle in the back has received it and ceases broadcasting. The assumption is that the vehicle in the back will be responsible for moving the message along to the rest of the platoon. Note that it is possible for a vehicle to receive a message more than once, forwarded by different vehicles in the front. If this happens, the vehicle only acts on the first message.

4.3 Mobicasting

A new spatiotemporary geocast routing protocol, called mobicast protocol has recently been proposed by Chen et al. [36] for VANET. Unlike conventional geocast routing protocol, the mobicast routing protocol takes the factor of time into account. The main goal of the mobicast routing protocol is the delivery of information to all nodes that happen to be in a prescribed region of space at a particular point in time. The mobicast protocol is designed to support applications which require spatiotemporary coordination in vehicular ad hoc networks. The spatiotemporary character of a mobicast is to forward a mobicast message to vehicles located in some geographic zone at time t, where the geographic zone is denoted as the Zone Of Relevance (ZOR_t). Vehicles located in ZOR_t at the time t should receive the mobicast message. As mentioned previously, VANET applications can be categorized into safety and comfort applications. Two features are introduced in the mobicast routing protocol for safety and comfort applications as follows.

To support safety applications, the mobicast routing protocol must disseminate the message on time. Vehicles located in the ZOR_t should receive the mobicast message before time $t + 1$; therefore, vehicles located in ZOR_t at time t must keep the connectivity to maintain the real-time data communication between all vehicles in ZOR_t. However, the connectivity in ZOR_t is easily lost if any vehicle in ZOR suddenly accelerates or decelerates its velocity, and this leads to a temporary network fragmentation problem. Some vehicles in ZOR_t cannot successfully receive the mobicast messages due to the temporary network fragmentation. To solve this problem, Chen et al. [36] present a new mobicast protocol to successfully disseminate mobicast messages to all vehicles in ZOR_t via a special geographic zone, known as Zone Of Forwarding (ZOF_t). This protocol dynamically estimates the accurate ZOF_t to guarantee that the mobicast messages can be successfully disseminated before time $t+1$ to all vehicles located in ZOR_t.

In contrast, comfort applications for VANET are usually delay-tolerant. That is, messages initiated from a specific vehicle at time t can be delivered through VANETs to some vehicles within a given constrained delay time λ. Chen et al. [37] further investigated a mobicast protocol to support comfort applications for a highway scenario in VANETs. For all vehicles located in the zone of relevance at time t (denoted as ZOR_t), the mobicast routing is able to disseminate the data message initiated from a specific vehicle to all vehicles which have ever appeared in ZOR_t at time t. This data dissemination must be done before time $t + \lambda$ through the multihop forwarding and carry-and-forward techniques. The temporary network fragmentation problem is also considered in their protocol design. A low degree of channel utilization should be maintained to reserve the resource for safety applications.

4.4 Quality of Service (QoS)

The term Quality of Service (QoS) is used to express the level of performance provided to users. High levels of QoS in traditional networked environments can often be achieved through resource reservation and sufficient infrastructure, however, these cannot be guaranteed in dynamic, ad-hoc environments, such as those used in VANETs due the VANETs inherent lack of consistent infrastructure and rapidly changing topology. Most QoS routing strategies aim to provide robust routes among nodes and try to minimize the amount of time required to rebuild a broken connection. However, factors such as node velocity, node positioning, the distance between nodes, the reliability of and delay between links can seriously affect the stability of a particular route. In their paper, Biswas et al. [35] introduced LDM-STREAM, a signalling mechanism of spatial divided network conditions to guarantee QoS in a VANET. It guarantees QoS by

detecting redundant source nodes and preventing the transmission of duplicate information thereby restricting redundant broadcasts that limit the application's bandwidth consumption and in so doing improves the latency of messages. LDM-STREAM can pick the most relevant data to transmit and the available bandwidth can be used in the most optimal way. Zhu et al. [38] analyzed some of the most important QoS metrics in VANETs using a comprehensive and realistic simulation testbed. Simulations were carried out in both highway and urban environments with varying vehicle density and speed to determine the upper performance bound for connection duration, packet delivery ratio, end-to-end delay, and jitter for unicast communication in typical highway and urban VANET environments. According to their results, delay and jitter in VANETs were adequate for most of the envisioned unicast-based applications, whereas the packet delivery ratio and connection duration may not meet the requirements for most unicast-based applications. Zhao et al. [39] simulated vehicles in an urban environment to analyze the performance of a multipath routing protocol and its impact on global QoS metrics. Their simulations show substantial improvement in performance compared to no multipath, only gateways multipath, only nodes multipath and all multipath when considering global QoS metrics in vehicle-to-vehicle and vehicle-to-infrastructure communications.

4.5 Security

The security of VANETs is crucial as their very existence relates to critical life threatening situations. It is imperative that vital information cannot be inserted or modified by a malicious person. The system must be able to determine the liability of drivers while still maintaining their privacy. These problems are difficult to solve because of the network size, the speed of the vehicles, their relative geographic position, and the randomness of the connectivity between them. An advantage of vehicular networks over the more common ad hoc networks is that they provide ample computational and power resources. For instance, a typical vehicle in such a network could host several tens or even hundreds of microprocessors [7]. Raya et al. [1] classify attackers as having three dimensions: "insider versus outsider", "malicious versus rational", and "active versus passive". The types of attacks against messages, can be described as follows: "Bogus Information", "Cheating with Positioning Information", "ID disclosure", "Denial of Service", and "Masquerade". The reliability of a system where information is gathered and shared among entities in a VANET raises concerns about data authenticity. For example, a sender could misrepresent observations to gain advantage (e.g., a vehicle falsely reports that its desired road is jammed with traffic, thereby encouraging others to avoid this route and providing a less-congested trip). More malicious reporters could impersonate other vehicles or road-side infrastructure to trigger safety hazards. Vehicles could reduce this threat by creating networks of trust and ignoring, or at least distrusting, information from untrusted senders.

4.5.1 Threats to availability, authenticity, and confidentiality

Attacks can be broadly categorized into three main groups: those that pose a threat to availability, those that pose a threat to authenticity and those that pose a threat to driver confidentiality. The following sections present threats posed to each of the areas of availability, authenticity, and confidentiality.

4.5.1.1 Threats to availability The following threats to the availability of vehicle-to-vehicle and vehicle-to-roadside communication (including routing functionality) have been identified:

- **Denial of Service Attack**: DoS attacks can be carried out by network insiders and outsiders and renders the network unavailable to authentic users by flooding and jamming with likely catastrophic results. Flooding the control channel with high volumes of artificially generated messages, the network's nodes, onboard units and roadside units cannot sufficiently process the surplus data.
- **Broadcast Tampering**: An inside attacker may inject false safety messages into the network to cause damage, such as causing an accident by suppressing traffic warnings or manipulating the flow of traffic around a chosen route.
- **Malware**: The introduction of malware, such as viruses or worms, into VANETs has the potential to cause serious disruption to its operation. Malware attacks are more likely to be carried out by a rogue insider rather than an outsider and may be introduced into the network when the onboard units and roadside units receive software and firmware updates.
- **Spamming**: The presence of spam messages on VANETs elevates the risk of increased transmission latency. Spamming is made more difficult to control because of the absence of a basic infrastructure and centralised administration.
- **Black Hole Attack**: A black hole is formed when nodes refuse to participate in the network or when an established node drops out. When the node drops out, all routes it participated in are broken leading to a failure to propagate messages.

4.5.1.2 Threats to authenticity Providing authenticity in a vehicular network involves protecting legitimate nodes from inside and/or outside attackers infiltrating the network using a false identity, identifying attacks that suppress, fabricate,

alter or replay legitimate messages, revealing spoofed GPS signals, and impede the introduction of misinformation into the vehicular network. These include:

- **Masquerading**: Masquerading attacks are easy to perform on VANETs as all that is required for an attacker to join the network is a functioning onboard unit. By posing as legitimate vehicles in the network, outsiders can conduct a variety of attacks such as forming black holes or producing false messages.
- **Replay Attack**: In a replay attack the attacker re-injects previously received packets back into the network, poisoning a node's location table by replaying beacons. VANETs operating in the WAVE framework are protected from replay attacks but to continue protection an accurate source of time must be maintained as this is used to keep a cache of recently received messages, against which new messages can be compared.
- **Global Positioning System (GPS) Spoofing**: The GPS satellite maintains a location table with the geographic location and identity of all vehicles on the network. An attacker can fool vehicles into thinking that they are in a different location by producing false readings in the GPS positioning system devices. This is possible through the use of a GPS satellite simulator to generate signals that are stronger than those generated by the genuine satellite.
- **Tunneling**: An attacker exploits the momentary loss of positioning information when a vehicle enters a tunnel and before it receives the authentic positioning information the attacker injects false data into the onboard unit.
- **Position Faking**: Authentic and accurate reporting of vehicle position information must be ensured. Vehicles are solely responsible for providing their location information and impersonation must be impossible. Unsecured communication can allow attackers to modify or falsify their own position information to other vehicles, create additional vehicle identifiers (also known as Sybil Attack) or block vehicles from receiving vital safety messages.
- **Message Tampering**: A threat to authenticity can result from an attacker modifying the messages exchanged in vehicle-to-vehicle or vehicle-to-roadside unit communication in order to falsify transaction application requests or to forge responses.
- **Message Suppression/Fabrication/Alteration**: In this case an attacker either physically disables inter-vehicle communication or modifies the application to prevent it from sending to, or responding from application beacons.
- **Key and/or Certificate Replication**: Closely related to broadcast tampering is key management and/or certificate replication where an attacker could undermine the system by duplicating a vehicle's identity across several other vehicles. The objective of such an attack would be to confuse authorities and prevent identification of vehicles in hit-and-run events.
- **Sybil Attack**: Since periodic safety messages are single-hop broadcasts, the focus has been mostly on securing the application layer. For example, the IEEE 1609.2 standard does not consider the protection of multi-hop routing. However, when the network operation is not secured, an attacker can potentially partition the network and make delivery of event-driven safety messages impossible.

4.5.1.3 Threats to confidentiality Confidentiality of messages exchanged between the nodes of a vehicular network are particularly vulnerable with techniques such as the illegitimate collection of messages through eavesdropping and the gathering of location information available through the transmission of broadcast messages. In the case of eavesdropping, insider and/or outsider attackers can collect information about road users without their knowledge and use the information at a time when the user is unaware of the collection. Location privacy and anonymity are important issues for vehicle users. Location privacy involves protecting users by obscuring the user's exact location in space and time. By concealing a user's request so that it is indistinguishable from other users' requests, a degree of anonymity can be achieved.

4.5.2 Authentication with digital signatures

Authentication with digital signature is a good choice for VANETs because safety messages are normally standalone. Moreover, because of the large number of network members and variable connectivity to authentication servers, a Public Key Infrastructure (PKI) is an excellent method by which to implement authentication where each vehicle would be provided with a public/private key pair. Before sending a safety message, it signs it with its private key and includes the Certification Authority (CA) certificate. By using private keys, a tamper-proof device is needed in each vehicle where secret information will be stored and the outgoing messages will be signed. The large computational burden of verifying a digital signature for every received packet has led to an exploration for alternatives. A Timed Efficient Stream Loss-tolerant Authentication (TESLA) [40] where the sender signs messages using a symmetric signature algorithm and then broadcasts this message with the signature (but most importantly, not the key). A short time later, the sender broadcasts the key and instructs all that this disclosed key is not to be used in the future. Receivers cache the original message until the key is received and then verify the signature. Since this verification uses symmetric cryptographic primitives, it requires approximately 1000 times less computational resources than Elliptic Curve Digital Signature Algorithms (ECDSA) [41].

In the current IEEE 1609.2 proposal, messages are authenticated using the Elliptic Curve Digital Signature Algorithm scheme and each message also includes a certificate.

Note that to economize over-the-air bandwidth, it is possible for verifiers to cache the certificates and public keys of a signer. This might allow the signer to send certificates in a subset of data messages or in separate certificate-sharing messages [42].

An overview of VANET security can be found in [43]. Various consortia presently are addressing VANET security and privacy issues, including the Crash Avoidance Metrics Partnership (CAMP) Vehicle Safety Communications-Applications project, the Vehicle Infrastructure Integration (VII) project, the SeVeCom project, and others. As shown above, IEEE 1609.2 also addresses security services for VANETs. A key challenge that remains in securing VANETs is to provide sender authentication in broadcast communication scenarios.

5 VANET trials and recent deployments in the US, Japan, European Union

Considerable effort has been invested in experimenting with various aspects of VANET systems and architecture and these trials are continuing. To a considerable degree simulation complements the results of real-life industrial trials. However in the end, actual implementations are an essential and necessary part of the verification of the operation and accuracy of VANET systems.

In recent years, several intelligent transportation system initiatives and projects have been undertaken. For example, in 2006 the European Commission implemented a safety program which was designed to reduce road fatalities by 50% by 2010 as well as to improve the efficiency of traffic flows [44]. These research and development trials are in progress and can be considered to be "Phase 1" in the development of vehicular communications network trials. This phase represents an important step towards the goals of improving road safety and traffic efficiency as well as providing Internet services to vehicles.

Early developments focused on the underlying wireless protocol infrastructure and included physical and MAC protocol standardization such as IEEE 802.11p, WAVE and DSRC. Subsequent developments and testing involve the messaging systems and overlaying application architectures.

Various projects (as shown in Fig. 6) are underway and several consortia have been established to demonstrate real-life VANET implementations and this can be considered to be "Phase 2" of research and development in VANETs. In this phase standardization and field trials are playing a vital role in the verification of the protocols and architectures developed during Phase 1.

Several consortia involving organizations such as the automotive industry, highway control authorities, toll service providers and safety organisations are now involved in this phase. To a considerable degree these trials have been funded by governments of the USA, Japan, and the European Union. There are many national and international projects supported by government, industry, and academia devoted to these field trials. These include consortia such as the Vehicle Safety Consortium (VSC) in the USA, Car-to-Car Communications Consortium (C2C-CC) sponsored by the European Union and the Advanced Safety Vehicle Program (ASV) in Japan. Other field trial programs include standardization efforts such as IEEE 802.11p (WAVE), and the large-scale Vehicle Infrastructure Integration Program (VII) in the USA. The following sections provide a brief overview of recent and current key projects that have been, or are in progress, under the auspice of agencies in USA, Europe, and Japan. Figure 6 provides a brief summary of these various projects.

5.1 USA

5.1.1 Wireless Access in Vehicular Environments (WAVE) (2004)

The Wireless Access in a Vehicular Environment (WAVE) software suite of standards were released and demonstrated in 2004 and further revised in 2006 [45]. This enabled practical trials of Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications to be demonstrated and the corresponding performance measured. This trial then became the foundation for further developments trials for the IVI, VSC and VII program trials described below.

5.1.2 Intelligent Vehicle Initiative (IVI) (1998–2004)

The goal of the Intelligent Vehicle Initiative (IVI) program [46] was to help prevent or reduce the severity of crashes through technologies that help drivers to avoid hazardous mistakes. More specifically, the objectives of the program were to (i) develop technology to assist in preventing driver distraction and (ii) facilitate accelerated development and deployment of crash avoidance systems.

5.1.3 Vehicle Safety Communications (VSC) (2002–2004), (VSC-2) (2006–2009)

The Vehicle Safety Communications (VSC) consortium [47] has run a set of trials over the last four years in coordination with the Highway Traffic Safety Administration. In particular the research and development being carried out under VSC-2 can be considered as "work in progress" with the objectives of the trials being to:

- Assess how previously identified critical safety scenarios can be improved by the use of DSRC along with positioning systems.

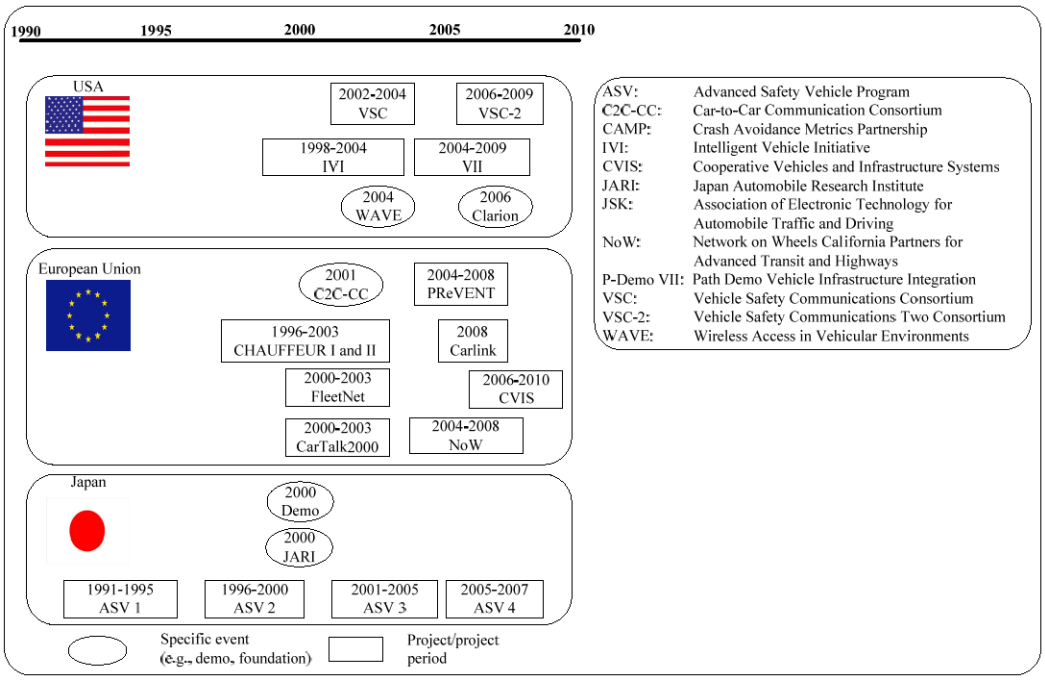

Fig. 6 VANET Trials supported by consortia in the USA, European Union, and Japan [42]

- Determine the minimum system requirement and associated performance parameters for vehicle safety applications operating in conjunction with this DSRC system.
- Implement deployment models for selected communications-based vehicle safety systems.

The work of VSC-2 seeks to implement a common vehicle safety communication architecture, (including protocols, messaging systems and interfaces) necessary to achieve interoperability among different vehicle manufacturers. Further, this work includes the implementation and verification testing of vehicle positioning technology in conjunction with DSRC to support a variety of safety applications.

5.1.4 Vehicle Infrastructure Integration (VII) (2004–2009)

The Vehicle Infrastructure Integration (VII) Consortium provides coordination between key automobile manufacturers (Ford, General Motors, Daimler-Chrysler, Toyota, Nissan, Honda, Volkswagen, BMW), IT suppliers, U.S. Federal and state transportation departments, and professional associations. The VII test environment covers 50 square kilometers near Detroit, USA and is used to test a variety of prototype VII applications [48]. The specific applications currently under development include:

- Warning drivers of unsafe conditions and imminent collisions.
- Warning drivers should they be about to run off the road.
- Providing real-time information to system operators concerning congestion, weather conditions, and other potentially hazardous incidents.
- Providing operators with real-time information on corridor capacity.

Other USA-based trials include the Clarion project [49] which is based on a consortium of Japanese and USA-based hi-tech vehicle technology companies and incorporates a small-scale version of a selection of the VSC and VII trials described above.

5.2 European Union (EU)

5.2.1 Car-to-Car Communications Consortium (C2C-CC)

The Car2Car [50] communication group is an organization comprising European vehicle manufacturers that is open for providers, research associations and other partners. The Car2Car Communications Consortium (C2C-CC) started trials in 2001 and demonstrated the use of IEEE 802.11 WLAN technologies in order for the vehicles to communicate with each other within the range of a few hundred meters.

The Car2Car communication trials are based on the following systems:

- Driver assistance using new wireless technologies.
- Design and development of active safety applications.

- Floating car data which operates by updating the service center which holds data relating to individual vehicles' parameters.
- User communication and information services.

C2C-CC also has the objective of contributing to the European standardization bodies and in particular ETSI TC ITS (European Telecommunications Standards Institute: Technical Committee: Intelligent Transport Systems). In addition, C2C-CC is a key contributor to the V2V and V2I validation trial processes.

5.2.2 *FleetNet (2000–2003)*

Fleetnet [51] was an early EU sponsored trial which built on the results of simulation experiments and a software prototype called FleetNet Demonstrator [52]. The objective was to identify problems inherent in inter-vehicular communication in a realistic VANET operation. The trial focused on how mobility could be achieved using position-based routing protocols using a set of six vehicles. Each vehicle had two on-board computers, one for handling the V2V and V2I communication through a wireless interface. The other system provided a graphical user interface for vehicular communication as well as communication with GPS receivers. The trial evaluated results of vehicular behavior in both highways and city environments and carried out appraisal of data transmission performance, velocity and distances amongst vehicles.

5.2.3 *Network on Wheels (NoW) (2004–2008)*

The Network on Wheels (NoW) [53] project and trial was founded by the automobile manufacturers (Daimler, BMW, Volkswagen), the Fraunhofer Institute for Open Communication Systems, NEC Deutschland GmbH and Siemens AG in 2004. NoW is a German research project which is supported by the Federal Ministry of Education and Research. In addition to the partners above, the Universities of Mannheim, Karlsruhe and Munich have all contributed to NoW trials. This is an initiative of the major European car manufacturers and suppliers with objectives to solve technical key issues on communication protocols and data security for car-to-car communications and to submit results to the standardization activities of the Car2Car Communications Consortium. The communications protocols developed in NoW support both active safety and infotainment applications and are providing an open communication platform for a broad spectrum of applications.

5.2.4 *PReVENT (2004–2008)*

PReVENT [54] was a EU sponsored project covering the period 2004–2008 and consisted of a set of trials which demonstrated safety applications using sensors, maps, and communication systems. The PReVENT trial [55] consisted of 23 cars, trucks, and different types of devices for evaluating active safety including:

- Safe speed and safe following distance.
- Collision control and intersection safety.
- Lateral support—which deals with applications focusing on keeping vehicles in their lanes as well as warning drivers if they are about to leave the road.
- Development of the ADAS Advanced Driver Assistance System (ADAS)[2] combined with mapping and GPS location systems.

5.2.5 *Cooperative Vehicles and Infrastructure Systems (CVIS) (2006–2010)*

CVIS is another EU-sponsored current project trial with the objective of increasing road safety [56]. CVIS tests technologies to permit vehicles to communicate with each other (V2V) and nearby roadside control points (V2I). The project commenced in 2006 and is planned to be completed by the end of 2010. CVIS manages traffic control systems and implements a variety of driver routing systems to take account of hazardous conditions. The main objectives of this trial are to develop standards for V2V and V2I communication and provide greater precision in vehicle location as well as the generation of more dynamic and accurate mapping using recent location referencing methods such as satellite navigation. The trials also address systems for cooperative traffic and network monitoring in both vehicle and roadside infrastructure along with the ability to detect potentially dangerous incidents. Further, it deploys a "floating car data" application which operates by updating the service center with individual vehicles' operational parameters.

5.2.6 *Car Talk 2000 (2000–2003)*

Car talk 2000 [57] was a 3 year project run within the 5th framework program of the EU and built on the earlier work of the US sponsored CHAUFFEUR trials [58].

The trial developed reliable components for Advance Driver Assistance (ADAS) such as Advanced Cruise Control (ACC) and to some degree overlaps with the work of the CVIS project described above. This project focused on three key aspects:

- Information and warning functions including traffic load, driving conditions, and road accident notifications.
- Communication-based longitudinal control systems which addressed collision avoidance systems affecting vehicles both in front and behind.

[2] ADAS is a term used in many VANET trials and covers a wide range of safety systems including: navigation, floating car data, collision avoidance systems, car-to-car communication, night vision safety, and others.

A list of other European Union supported trials up to and including 2008 are described in [59].

5.3 Japan

5.3.1 Advanced Safety Vehicle Program (ASV-2) (1996–2000), (ASV-3) (2001–2005), (ASV-4) (2005–2007)

The Advanced Safety Vehicle Program (ASV) program has been a series of ongoing development projects covering various trial phases and was supported by the Japanese Ministry of Transport, automobile manufacturers (Honda, Mitsubishi, Suzuki and Toyota in particular) as well as academic and research organisations. The trials focused on two aspects of safety—active and passive. In the active safety trial, systems were tested which addressed inattention and driver errors. In particular these relate to drowsiness warning systems, vision enhancement systems, navigation systems, automatic collision avoidance systems and lane departure systems. The passive systems included impact absorption systems, occupant protection systems, pedestrian protection systems and door lock sensing systems.

5.3.2 Demo 2000 and JARI (Japan Automobile Research Institute)

Two earlier demonstration trials of significance were Demo 2000 [60] and JARI [61]. The Demo 2000 project described demonstrations of a cooperative driver assistance system. They evaluated the feasibility and technologies necessary for inter-vehicle communications. The Dedicated Omni Purposed Inter-vehicle link protocol was used in 5.8 GHz band employing Digital Cellular Radio Communication and Carrier Sense Multiple Access medium access control protocols. Each vehicle was equipped with laser radar for the measurement of distance, obstacles, and liquid crystal displays for displaying vehicle communication. Closely related are the trials supported by JARI which evaluated the technologies found in many parallel trials being carried out in the USA and the European Union involving intelligent vehicles, collision avoidance, and safety systems.

6 VANET simulation models, tools, and platforms

The environment and topology of VANETs makes it difficult to implement and evaluate them. Outdoor experiments can be used to evaluate VANET protocols and applications but these can be difficult and expensive to implement because of the high number of vehicles and real-life scenarios involved. It is difficult to perform actual empirical performance measurements because of the inherently distributed, complex environment. To overcome these limitations, simulation tools are used extensively for VANET simulations.

6.1 Mobility models for VANETs

In contrast to existing VANET simulation models, which treat all nodes identically, [62] have developed a role based mobility model that can differentiate nodes by their roles, allowing nodes to have different roles and to have strategies based on both micro and macro mobility scope. Results show that the common problem of unrealistic traffic patterns and situations that do not reflect real-life can be overcome using this role-based mobility model. However, this simulation model has some limitations in that it is incapable of simulating complex traffic elements such as overpasses, bridges and tunnels. Liu et al. [63] propose a wireless network VANET simulation tool called VGSim, an integrated networking and microscopic vehicular mobility simulation platform that can accurately model traffic mobility. The developers of VGSim believe that their product fulfils most of the requirements of an accurate simulation, namely closed-loop integration of realistic vehicular traffic and a wireless communication simulation module. They argue that VGSim is highly flexible, and more resource efficient compared to similar approaches and can easily adopt different mobility models.

To achieve good results from VANET simulations, we need to generate a mobility model that is as realistic as an actual VANET network. Different types of mobility models (a mobility model defines the set of rules that defines the movement pattern of nodes used by network simulators to create random topologies based on nodes position and perform some tasks between the nodes.) have been used in VANET simulations. We classify them according to the level of details they generate.

One challenge associated with mobility models applied to VANETs is the separation of a mobility model at the Macroscopic and Microscopic level [64]. A mobility model includes some constraints like streets, lights, roads, buildings, cars, vehicular movements and inter-vehicle behavior. These constraints are divided into two parts: the node mobility part includes streets, lights, roads, buildings etc. and is classified as Macroscopic, whereas the movement of vehicles and their behaviors are classified as Microscopic. We can also view the mobility model as one that includes a *Traffic generator* and a *Motion generator*. Motion constraints are designed by car driver habits, cars and pedestrians and describe each vehicle movement. The *Traffic generator* creates random topologies from maps and defines the vehicular behavior under environment. It is also worth mentioning that a mobility model is also described by a framework that includes topological maps such as lanes, roads, streets, obstacles in mobility, communication model, car velocities based on traffic densities related to how the simulation time could be varied, vehicular distribution on roads and intelligent driving pattern. The illustration of this framework is given in Fig. 7.

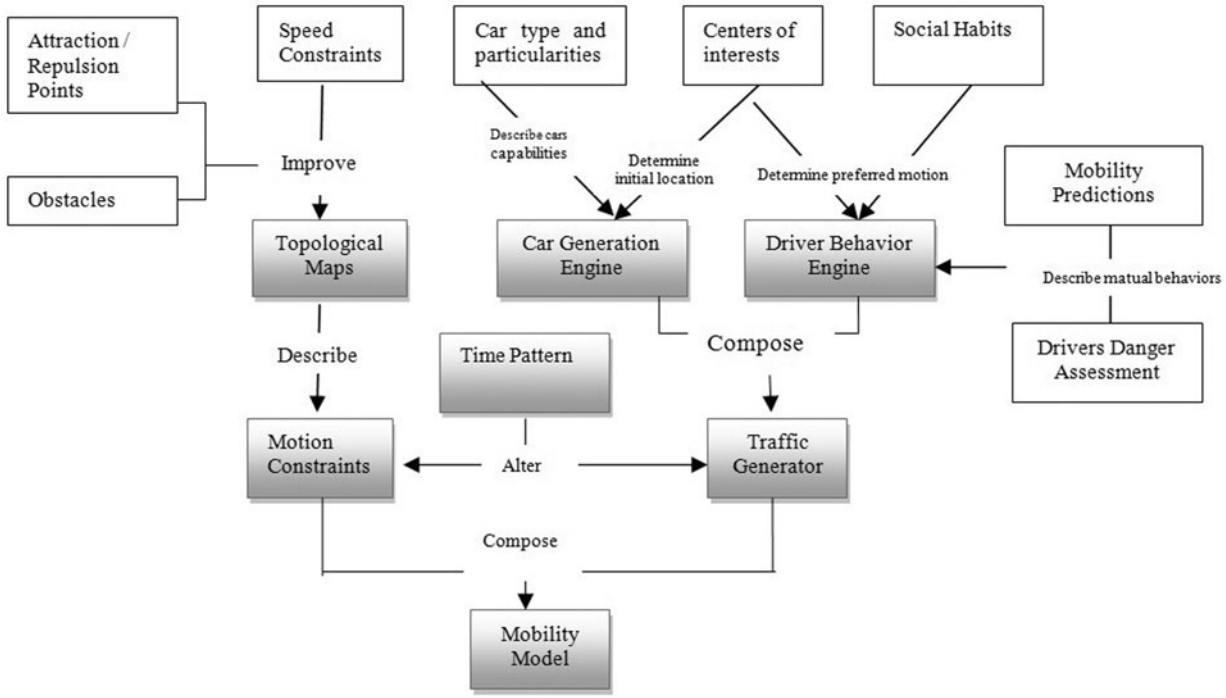

Fig. 7 Mobility model [65]

To perform VANET simulation tests, a mobility model must be generated. One way of capturing a realistic model would be to generate patterns from mobility traces. In recent years, many researchers have tried to refine existing mobility models in order to make them more realistic by exploiting the available mobility traces [66]. The main idea behind such models is the use of available measurements (e.g., connectivity logs) to generate synthetic traces that are characterized by the same statistical properties of the real VANET scenarios. We present a few models that generate traces that are used by mobility models.

6.1.1 Survey models

Survey models represent realistic human behavior in urban mesh environments. The model relies on data collected through surveys performed on human activities. One of the large surveys [67] came from US Department of Labor, which performed a survey by recording the workers behavior and their activities at lunch time, communicating with them, pedestrians, lunch and break time etc and collected the statistics, which later on helped in creating a generic mobility model. The survey was recorded for the human performance, tasks, and activities. For example, the UDel mobility model [68] is a tool for simulating urban mesh networks. The UDel model includes obstruction in mobile nodes and generates a graph of the urban area. The mobile nodes are then placed on the graph and their behavior is observed.

6.1.2 Event driven models

Event driven models, also called trace models, can be used to monitor the movement of human beings and vehicles, analyzing them and generating traces based on their mobility. In [65], the authors presented a WLAN mobility model, in which the traffic characteristics of WLAN users were measured across the campus. In [69], the authors observed how WLAN users connect with an infrastructure network.

Event driven models could be gathered to develop a probabilistic mobility model that reflects the real movement on the map. This probabilistic mobility model helped to develop a discrete event Markov chain, which considered the source, destination paths, and the current and previous location. The problem with this model is that only the characteristics of mobile nodes with access points were considered; no relationship between the nodes was considered. As a result, probabilistic models cannot support the ad hoc mode of VANET.

6.1.3 Software oriented models

Various simulators such as VISIM [70], CORSIM [71] and TRANSIM [72] are able to generate the traces of urban microscopic traffic. VanetMobiSim [73] uses the [74] database and Voronoi graphs [75] to extract road topologies, maps, streets and other details for the network simulators. The

problems with such simulators are that they can only operate at traffic level and they cannot generate realistic levels of details. Moreover the inter-operability with other network simulators and the generated level of details are insufficient for other network simulators.

6.1.4 Synthetic model

A lot of work has been carried out in the area of synthetic modeling. All models in this category use mathematical equations to develop realistic mobility models. The strength of mathematical models is validated by comparing them with real mobility models. According to [76] synthetic models can be divided into 5 main categories:

- Stochastic model: deals with totally random motion.
- Traffic Stream model: examines the mechanical properties of mobility model.
- Car Following model: monitors the behavior of car-to-car interaction.
- Queue model: considers cars as standing in queues and roads as queue buffers.
- Behavioral models: examines how movement is influenced by social interaction.

For example if we consider a mobile node in an area and observe its movement, it can either move in a fixed line or it could follow a random path. The Weighted Way Point (WWP) (the destination is chosen on the basis of current location and time) and the Random Way Point (RWP) (the destination is chosen randomly) mobility algorithm calculate the mobility pattern of a node by defining certain mathematical equations. The synthetic model imposes certain limitations such as excluding a real human behavioral model. As a result, it is difficult to create random topologies with this model.

6.2 Evaluation of VANET simulators

Many simulators exist for VANET but none of them can provide a complete solution for simulating VANETs. This is mainly because VANET relies on and is related to two other simulations for its smooth functioning, namely traffic simulation and network simulation. *Traffic simulators* are used for transportation and traffic engineering. *Network simulators* are used to evaluate network protocols and application in a variety of conditions. These simulators work independently. To satisfy the need of VANET, a solution is required that uses these simulators together. Numerous traffic and network simulators have attempted to address the simulation of VANET but each solution has had its shortcomings. There are many traffic and network simulators but they need to interact with each other to evolve into what can be called a VANET simulator. The issue still remains as to why these two simulators cannot inter-operate. One strong reason is the mismatch in formats. In many cases, the format of mobility models generated by the traffic simulator cannot be processed by the network simulator. For example, network simulators such as NS-2 cannot directly accept trace files from other traffic simulators.

Various commercial traffic level simulators such as AIMSUN [77], VASIM [78], CORSIM [71] exist with strong Graphical User Interface support and support various traffic level features. But they are fairly expensive (for example, the acquisition of a single license for these commercial software starts from 9,000 US dollars) and because of their proprietary nature we cannot have source code access limiting the ability of researchers to make modifications. In addition, these simulators also generate lots of details not yet intended to be used by traditional popular network simulators. An evaluation of commercial traffic simulators is beyond the scope of this paper since a complete review is already presented in [79]. Instead, we will focus on freeware simulators given their availability and access to their source code for any modifications by users.

Several mobility models such as the Gauss-Markov model, Random walk model, node following model, Platoon, Random Waypoint model are used to generate node mobility features including velocity variation, random movement within a topology boundary, etc. Among all these models, the Random Waypoint model is widely used but the mobility patterns it generates does not match node behavior in the real world. Hence the scientific community focused on other projects, starting from the generation of simple to more complex mobility patterns. Unfortunately these projects were more geared towards the traffic side; only a small amount of work had been done on the network side.

To qualify as a candidate for VANET simulator, the candidates must satisfy both the *traffic level* and *motion level* criteria. The traffic level is concerned with details such as streets, obstruction in communication paths, lights and vehicular densities. For the simulation to capture details at traffic level, it must include the following information movement topologies (custom, random, maps graphs), start and end position, trip through different positions, selection of track, speed of vehicles. After all the details at the traffic level have been captured, the motion level criteria are used to create topologies between the nodes and analyze their behavior based on the details gathered at traffic level (e.g., a car may change its lane and try to overtake). It also monitors the situation during heavy traffic flow or vehicles standing in line and following each other. Models are also adopted from mathematical equations that produce all possible vehicular behavior patterns. There are various models that fall under this category. The most widely used model is the "car following model". This is a widely used model

which describes the process of vehicles following each other in the same line. This model been preferred over other traffic models such as Krauss Model (KM) [80], General Motors Model (GM), Gipps Model (GP) [81], Intelligent Driver Model (IDM).

It would also be appealing if the VANET simulator also supports a Graphical User Interface (GUI). Furthermore, while simulating real world complex scenarios the simulator must also consider the approach to simulate radio obstacles in the wireless communication medium. In addition, the VANET simulator should also be able to generate trace files for other simulators such as NS-2 or QualNet. The following simulators satisfy the above criteria (traffic level and motion level): MOVE [82], Trans [83], VanetMobiSim [73], NCTUns [84].

Simulators such as CanuMobiSim [85] has been designed to generate only traffic level details but has limited capability to generate motion level details unlike MOVE and NCTUns simulators. The following simulators generate details at the network level: NS [86], GlomoSim [87].

6.2.1 *MObility model generator for VEhicular networks (MOVE)*

MOVE (The MObility model generator for VEhicular networks (MOVE) is a Java-based application built on SUMO (Simulation of Urban Mobility) [88] with GUI support. MOVE supports a very good visualization tool and focuses mainly on traffic level features. In addition, it also supports custom graphs defined by the user as well as random generated graphs. But with random generated graphs, it restricts the node movement to a grid (i.e., the node should only move on the grid). MOVE is composed of a Map editor and a Vehicular Movement editor. The Map editor creates topological maps for network scenarios and the vehicular movement editor generates movement patterns automatically or use those defined by the users in the editor. MOVE can also generate its own mobility model but the results obtained are not satisfactory as compared to that of standard mobility models. The problem accompanied with this mobility model is the lack of support for large networks (i.e., its packet delivery ratio drops as the number of nodes increases). Moreover multiple radio interfaces are not supported by larger networks [82].

While generating mobility traces, MOVE takes micro-mobility into consideration. The micro-mobility feature does not include any Lane-changing or Obstacle mobility models. The intersection management follows a simplistic stochastic model [76] and therefore random movement of a node in the topology is not considered. MOVE utilizes the federated approach, in which they both communicate via a parser. The traces from the traffic simulators are sent to the parser for translation and then processed by the network simulator. The updated file from the network simulator is passed to the traffic simulator via the parser. The problem with this approach is that the interaction between the two simulators is not done in a timely manner.

6.2.2 *Traffic and network simulator (TraNs)*

TraNS is a Java-based application with a visualization tool that was built to integrate SUMO and NS-2 specifically designed with VANET simulation in mind. SUMO translates the traffic file to some form of a dump file which is later used by a network simulator. However TraNs has also developed a stepped down version called TraNs Lite for the purpose of generating a mobility model only, without using integrated NS-2 simulators for the network simulation. TraNs lite is a scalable software with the ability to simulate up to 3,000 nodes and can extract mobility traces using Shapefile (A vector map, with points, polylines and polygons) and these maps could be cropped down according to the user's specification. The problem with the TraNs architecture is that the output obtained from NS-2 cannot be passed back to SUMO (i.e., NS-2 generates its output to *file.out* file and during VANET simulation, this *file.out* cannot be passed to SUMO for regeneration of traces. Thus, the two loosely coupled simulators fail to produce results that are similar to real life examples.

6.2.3 *VanetMobiSim*

VanetMobiSim is an extension to CanuMobiSim. Given the limited scope of CanuMobiSim to be used in specific areas only, VanetMobiSim cannot produce high levels of details in specific scenarios. Therefore CanuMobiSim was extended to achieve a high level of realism with VanetMobiSim. Modeling of VanetMobiSim includes car-to-car and car-to-infrastructure scenarios. Thus it combines stop signs, traffic lights, and activity-based macro-mobility with human mobility dynamics. It can extract road topologies from random and custom topologies. It allows users to generate trips based on their own assumptions and can configure the path between the source and destination based on Dijkstra algorithm, road-speed shortest, or density-speed shortest. VanetMobiSim contains a parser to extract topologies that can be used by network simulators. The main problem with the VanetMobiSim approach is that the traces generated by VanetMobiSim cannot be fed back to the network simulator or the traces generated by network simulator cannot be used as input to VanetMobiSim. For the VANET Simulation to work effectively the two simulators should cooperate with each other to give successful simulation results. VanetMobiSim does not work well with network simulators to achieve the goals for VANET Simulation.

Table 3 Traffic and Motion level features of SUMO, MOVE, TranNs, VanetMobiSim, and NCTuns simulators

Attribute	SUMO/MOVE/TraNs	VanetMobiSim	NCTuns
Custom Graphs	Supports	Supports	Supports
Random Graphs	Grid Based	Voronoi Graphs	SHAPE-File
Graphs from Maps	TIGER database	GDF	Bitmap image
Multilane Graphs	Support	Support	Support
Start/End position	AP, Random	AP, Random	Random
Trip	Random Start—End	Random Start—End	Random
Path	Random Walk, Dijkstra	Random Walk, Dijkstra	Random Walk
Velocity	Road Dependent, Smooth	Road Dependent, Smooth	Road Dependent, Smooth
(a) Traffic level features			
Human Patterns	Car Following Models	Intelligent driver model, Intelligent driver model with intersection management, Intelligent driver model with Lane changes	Intelligent driver model with car following, Intelligent driver model with Lane changing, Intelligent driver model with intersection management
Intersection Management	Stoch turns	Traffic lights and signs	Traffic lights
Lane changing	No Support	MOBIL [90]	Supports
Radio Obstacles	No Support	Supports	Supports
(b) Motion level features			
Supports GUI	Yes	Yes	Yes
Output	ns-2, GlomoSim, QualNet	ns-2, GlomoSim,	NS-2
Other features	Federated / Integrated	Separate	Integrated

6.2.4 National Chiao Tung university network simulator (NCTUns)

NCTUns [84] is written in C++ with a powerful GUI support. NCTUns can simulate 80.211a, 802.11b, 802.11g and 802.11p technologies. NCTuns can simulate multiple wireless interfaces inside one node including 802.11.p interface. After the release of version 5 [89], NCTuns enhanced its usability for ITS. NCTuns includes free space with a shadowing path loss model, Rayleigh and Ricean fading models. NCTUns implements directional, bidirectional and rotating antenna types. The Signal to Noise Ratio calculation is cumulative and the signal strength is determined from the sender's and receiver's perspective point. NCTUns implements block objects to introduce the hindering object between wireless signals. The Wall object can completely block the wireless signal or can attenuate the signal with a specified value. The hindering object gives good simulation environment to observe the effects of multi hop wireless network simulation. During the simulation, each node is allowed to send either a UDP or TCP packet. However, there is a limitation in NCTUns. Most of the Network simulators allow multiple TCP/IP versions (Tahoe and New Reno) inside single simulators whereas NCTUns allows only a single instance of TCP/IP version. Unlike TraNs, NCTUns which integrate traffic and network simulators within a single module with a powerful feedback to support vehicular network simulations. As we mentioned earlier, the feedback between the traffic and the network simulators in a timely manner is needed for efficient VANET simulations. Thus, NCTUns is the only simulator that overcomes the limitations of other simulators discussed earlier namely MOVE, TraNS, and VANETMobiSim. However, NCTUns can support a maximum of only 4096 nodes inside a single simulation.

We summarize in Table 3 below the main attributes for traffic-level and motion-level features for SUMO, MOVE, TranNs, VanetMobiSim, and NCTuns.

Finally, to conclude, Fig. 8 depicts the strength of the various simulators discussed above in particular those related to VANET simulations.

7 VANET research challenges

In this section, we discuss some of the VANET-related research challenges that still need further investigation and innovative solutions to enable VANET infrastructures, communications, security, applications, and services.

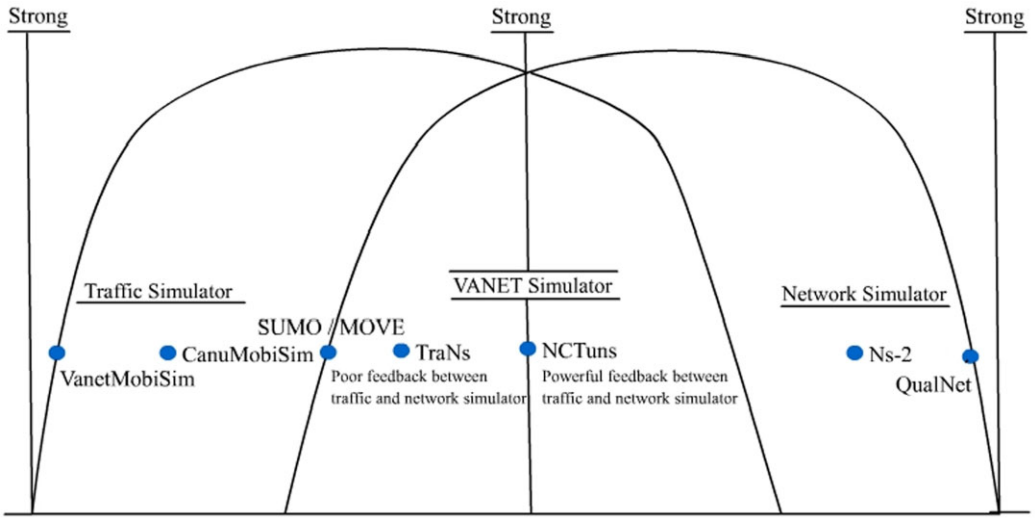

Fig. 8 Strength of traffic, VANET, and network simulators

7.1 Routing protocols

Routing plays an important role in VANET applications but the high-speed mobility of vehicles and their rapidly changing topology results in conventional MANET routing protocols being inadequate to efficiently and effectively deal with this unique vehicular environment as intermediate nodes cannot always be found between source and destination and end-to-end connectivity cannot always be established. This has prompted researchers to find scalable routing algorithms that are robust enough for the frequent path distributions caused by vehicle mobility [91, 93, 94], new and novel approaches that can deliver improved throughput and better packet delivery ratio [3, 4]. Sun et al. [91] propose a novel vehicular ad hoc routing protocol that utilizes both Zone Routing Protocol (ZRP) and Global Positioning Information (GPSR). Using the history cache to store the movement information of intra-zone vehicles and destination location information, the proposed routing protocol can predict an efficient path. By applying GPSR function on ZRP border nodes only (and not for all of its neighbors), better routing performance can be achieved for VANETs. Chung et al. [93] address the problem of spectrum access to deal with channel dynamics due to highly mobile nodes. A multi-channel Media Access Control (MAC) design that supports concurrent transmissions by allocating the channel for every beacon interval, is inadequate for fast-fading VANET environments. In contrast, a MAC design based on opportunistic spectrum access that selects a channel for each transmission cannot provide fair share of spectrum among devices. To address deficiencies of these MAC designs, Chung et al. [93] present the design and evaluation of a Cognitive MAC for VANET (CMV). CMV utilizes both long-term and short-term spectrum access, which not only provides a fair share but also exploits multi-user diversity, while achieving a significant increase in the overall network throughput. Their results show that CMV improves previous multi-channel MAC protocols throughput by up to 72% when compared with traditional dedicated and split protocols. Okada et al. [95] propose a novel selection scheme for the next-hop node in VANET. In their scheme, a new link metric called 'expected progress distance' is introduced in order to consider both forwarding distance and the transmission quality of the wireless link. They demonstrate that their approach can achieve much higher throughput and a better packet delivery ratio over existing conventional schemes such as greedy perimeter stateless routing, flooding-based geo-casting protocols, beaconless routing algorithms and contention-based forwarding. Yu and Ko [24] introduce a novel Delay/Disrupted Tolerant Network (DTN) routing scheme that uses a Message Ferry technique for VANETs. Geographic information is used to divide the road into blocks and control block size to ensure 1-hop communication between vehicles. Speed selection is designed for a minimum number of ferries and fast packet delivery. Simulation results show that their scheme has better delivery ratio when the delay is over 400 seconds and more messages are delivered to their destinations in the case of heavy load when compared with the Distance-Aware Epidemic Routing (DAER) scheme [92]. Although the initial results are promising, a more comprehensive simulation study must be conducted to verify the stability and superiority of their protocol for optimal end-to-end delays. In addition, different performance comparisons with other DTN protocols are also required to further demonstrate the performance efficiency of the proposed scheme. Ali and Bilal [94] propose a VANET routing protocol that is especially designed for city environments. It consists of the selection of the next junction dynamically and an intelli-

gent greedy strategy is used to forward packets between two junctions. The authors, inspired by the work of Jerbi et al. [96] proposed a geographical routing protocol using digital maps and vehicle density to select the next junction. Their work addresses some of the issues associated with the Improved Greedy Traffic Aware Routing (GyTAR) protocol [96] namely an intersection-based geographical routing protocol capable of finding robust routes within city environments. GyTAR, moves a packet successively closer to the destination along streets where there are enough vehicles to provide connectivity. Although GyTAR outperforms previous routing protocols in terms of packet delivery ratio, routing overhead, and end-to-end delay, GyTAR suffers large end-to-end delays and decreased packet delivery ratio when there are vehicles on the road opposite the direction of desired destination (such as one-way roads). Other issues such as the integration of VANETs with cellular networks, situation aware vehicular routing, and group formation still require further investigation.

7.2 Security frameworks

As we discussed above, efficient security support is an important requirement of VANETs. Several VANET security challenges still need to be addressed in the areas of authenticity, driver confidentiality, and availability. We need lightweight, scalable authentication frameworks that are capable of protecting vehicular nodes from inside and/or outside attackers infiltrating the network using a false identity, identifying attacks that suppress, fabricate, alter or replay legitimate messages, revealing spoofed GPS signals, and prevent the introduction of misinformation into the vehicular network. Early work in this area has been undertaken by Verma and Dihiang [97]. As far as driver confidentiality is concerned, we need reliable and robust secure protocols that can protect message exchanges among nodes of a vehicular network from threats such as unauthorized collection of messages through eavesdropping or location information (through broadcast messages). Choi and Jung [98] propose a prototype security framework aimed at mitigating threats to confidentiality in VANETs. To ensure availability, we also need mechanisms in place that can detect and mitigate attacks (such as Denial of Service) that can deny authenticated users access to the network. Some early works in this area is also presented in [97, 98].

Secure, efficient message exchange and authentication schemes operating for Vehicle-to-Infrastructure (V2I) and Vehicle-to-Vehicle (V2V) communications are required. For instance, mechanisms that can perform fast authentications between vehicles and roadside infrastructure units are needed to avoid delays. The use of a central, trusted authority and the use of public/private key-based solutions for vehicle-to-vehicle communication not only suffer high operational costs and response times but are also not scalable. We need to investigate innovative fast, low-cost message exchange solutions whose communication overheads remain constant as the number of vehicles in the communication range increases. We need novel encryption protocols that can operate at high speed compared to traditional public key-based solutions which incur more delays and overheads when encrypting messages from neighboring vehicles. The Secure Group Communications (SeGCom) scheme proposed in [97] is a lightweight solution that addresses some of these challenges for the V2V scenario by exploiting only one encryption method when creating and disseminating emergency messages. The authors in [98] proposed an ID-based cryptosystem (for safety-related applications) that implements strong repudiation and privacy while eliminating the overheads associated with certificate management prevalent in Public Key Infrastructure (PKI) systems. However, the use of a trusted third party to verify a vehicle's identifier may not lead to a scalable solution as mentioned previously.

7.3 Quality of service

Although current efforts [99] have attempted to optimize the available bandwidth to improve latency of messages, QoS support over VANETs remains a challenge because of the various factors we discussed earlier. We need to develop *adaptive QoS routing* approaches that can quickly and efficiently set up new routes when current routing paths becomes no longer available as a result of changes in node velocity, node positioning, network topology or distance between vehicular nodes. Well-defined QoS metrics for VANETs still need to be agreed upon given the wide variations of performance metrics (including popular QoS ones such as delay and jitter) being used by the VANET community. Initial results by Boban et al. [100] demonstrate that the real QoS challenges are packet delivery ratio and connection duration (rather than typical QoS metrics such as end-to-end delay and jitter [100]) are hard to achieve for unicast-based applications. Although multipath routing improves global QoS [101] metrics we need more in-depth research to investigate the impact of the multipath approach on the available bandwidth and processing load of intermediate vehicular nodes involved in the various paths used.

7.4 Broadcasting

Broadcasting continues to be a strong research area of focus by VANET researchers because a significant number of messages transmitted in VANETs are broadcast messages. Novel broadcasting algorithms are required to minimize broadcast storms that arise as a result of packet flooding. In addition, the underlying 802.11 wireless communication

technology used by VANET is not well suited at handling broadcast transmissions because of frequent message collisions leading to frequent retransmissions by vehicles. These collisions in turn affect the message delivery rate and increases the delivery time of the messages. Further research is required to investigate intelligent flooding schemes, distributed algorithms that can efficiently handle asymmetric communications among vehicles for different transmission ranges.

Providing *reliable* broadcast messages with minimal overheads for VANETs introduces several other technical challenges including: the selection of the next forwarding node, the maintenance of communications among vehicles as they leave and join a group, hidden terminal problems since broadcast messages do not use the typical Request to Sender/Clear to Sender (RTS/CTS) message exchange employed by IEEE 802.11.

Research proposals [102–104] have only recently begun to investigate broadcasting techniques for VANET but more research is required to enable highly efficient, reliable broadcasting techniques for VANET.

8 Conclusion

The convergence of computing, telecommunications (fixed and mobile), and various kinds of services are enabling the deployment of different kinds of VANET technologies. In the past decade, many VANET projects around the world have been undertaken and several VANET standards have been developed to improve vehicle-to-vehicle or vehicle-to-infrastructure communications. In this work, we reviewed some of the main areas that researchers have focused on in the last few years and these include security, routing, QoS, and broadcasting techniques and we highlighted the most salient results achieved to date. We presented a thorough analysis of various simulation tools that are available for VANET simulations. We hope this taxonomy on VANET simulators will be helpful to future VANET researchers in choosing the optimal VANET simulator best suited for their VANET design goals. Finally, we discussed some of the challenges that still need to be addressed in order to enable the deployment of VANET technologies, infrastructures, and services cost-effectively, securely, and reliably.

Acknowledgements The authors would like to express their deepest gratitude to Professor Tony Larsson for his guidance, support, and contributions on the VANET simulation section of this paper. Sherali Zeadally was supported partly by an NSF award (No. 0911969) and partly by a Visiting Erskine Fellowship from the University of Canterbury during this work.

References

1. Raya, M., & Hubaux, J. (2005). The security of vehicular ad hoc networks. In *Proceedings of the 3rd ACM workshop on security of ad hoc and sensor networks (SASN 2005)* (pp. 1–11), Alexandria, VA.
2. Harsch, C., Festag, A., & Papadimitratos, P. (2007). Secure position-based routing for VANETs. In *Proceedings of IEEE 66th vehicular technology conference (VTC-2007), Fall 2007* (pp. 26–30), September 2007.
3. Gerlach, M. (2006). *Full paper: assessing and improving privacy in VANETs*. www.network-on-wheels.de/downloads/escar2006gerlach.pdf (accessed: May 29, 2010).
4. Jinyuan, S., Chi, Z., & Yuguang, F. (2007). An ID-based framework achieving privacy and non-repudiation. In *Proceedings of IEEE vehicular ad hoc networks, military communications conference (MILCOM 2007)* (pp. 1–7), October 2007.
5. Stampoulis, A., & Chai, Z. (2007). *A survey of security in vehicular networks*. http://zoo.cs.yale.edu/~ams257/projects/wireless-survey.pdf (accessed: May 29, 2010).
6. Balon, N. (2006). *Introduction to vehicular ad hoc networks and the broadcast storm problem*. http://www.csie.ntpu.edu.tw/~yschen/course/96-2/Wireless/papers/broadcast-5.pdf (accessed: May 29, 2010).
7. Bickel, G. (2008). *Inter/intra-vehicle wireless communication*. http://userfs.cec.wustl.edu/~gsb1/index.html#toc (accessed: May 29, 2010).
8. Standard specification for telecommunications and information exchange between roadside and vehicle systems—5 GHz band dedicated short range communications (DSRC) medium access control (MAC) and physical layer (PHY) specifications. *ASTM E2213-03*, September 2003.
9. Notice of proposed rulemaking and order FCC 02-302. Federal Communications Commission, November 2002.
10. Kudoh, Y. (2004). DSRC standards for multiple applications. In *Proceedings of 11th world congress on ITS*, Nagoya, Japan.
11. Yin, J., Elbatt, T., & Habermas, S. (2004). Performance evaluation of safety applications over DSRC vehicular ad hoc networks. In *Proceedings of VANET'04*, Philadelphia, PA, USA, October 2004.
12. Jiang, D., & Delgrossi, L. (2008). IEEE 802.11p: towards an international standard for wireless access in vehicular environments. In *Proceedings of 67th IEEE vehicular technology conference on vehicular technology* (pp. 2036–2040), May 2008.
13. Festag, A. (2009). Global standardization of network and transport protocols for ITS with 5 GHz radio technologies. In *Proceedings of the ETSI TC ITS workshop*, Sophia Antipolis, France, February 2009.
14. IEEE Standard 802.11 (2007). IEEE Std. 802.11-2007, Part 11: wireless LAN medium access control (MAC) and physical layer (PHY) specifications.
15. IEEE P802.11p/D3.0, draft amendment for wireless access in vehicular environments (WAVE), July 2007.
16. IEEE Standard 1455-1999 (1999). IEEE standard for message sets for vehicle/roadside communications (pp. 1–130).
17. IEEE Standard 1609.1-2006 (2006). IEEE trial-use standard for wireless access in vehicular environments (WAVE)—resource manager (pp. 1–63).
18. IEEE Standard 1609.2-2006 (2006). IEEE trial-use standard for wireless access in vehicular environments—security services for applications and management messages (pp. 1–105).
19. IEEE Standard 1609.3-2007 (2007). IEEE trial-use standard for wireless access in vehicular environments (WAVE)—networking services (pp. 1–87).
20. IEEE Standard 1609.4-2006 (2006). IEEE trial-use standard for wireless access in vehicular environments (WAVE)—multichannel operation (pp. 1–74).
21. IEEE Standard 802.16-2004 (2004). IEEE standard for local and metropolitan area networks, part 16: air interface for fixed broadband wireless access systems.

22. Harsch, C., Festag, A., & Papadimitratos, P. (2007). Secure position-based routing for VANETs. In *Proceedings of IEEE 66th vehicular technology conference, VTC-2007, Fall 2007* (pp. 26–30), Baltimore, September 2007.
23. Sun, S., Kim, J., Jung, Y., & Kim, K. (2009). Zone-based greedy perimeter stateless routing for VANET. In *Proceedings of international conference on information networking, ICOIN 2009* (pp. 1–3), January 2009.
24. Yu, D., & Ko, Y.-B. (2009). FFRDV: fastest-ferry routing in DTN-enabled vehicular ad hoc networks. In *Proceedings of 11th international conference on advanced communication technology* (Vol. 2, pp. 1410–1414), February 2009.
25. Ali, S., & Bilal, S. (2009). An intelligent routing protocol for VANETs in city environments. In *Proceedings of 2nd international conference on computer, control and communication, IC4 2009* (pp. 1–5), February 2009.
26. Mohandas, B., & Liscano, R. (2008). IP address configuration in VANET using centralized DHCP. In *Proceedings of 33rd IEEE conference on local computer networks*, Montreal, Canada, October 2008.
27. Füßler, H., Mauve, M., Hartenstein, H., Käsemann, M., & Vollmer, D. (2002). *A comparison of routing strategies for vehicular ad hoc networks* (Technical report, TR-02-003). Department of Computer Science, University of Mannheim, July 2002.
28. Karp, B., & Kung, H. (2000). Greedy perimeter stateless routing for wireless networks. In *Proceedings of ACM international conference on mobile computing and networking (MobiCom 2000)* (pp. 243–254), Boston, MA, August 2000.
29. Basagni, S., Chlamtac, I., Syrotiuk, V., & Woodward, B. (1998). A distance routing effect algorithm for mobility (DREAM). In *Proceedings of ACM international conference on mobile computing and networking* (pp. 76–84), Dallas, TX, October 1998.
30. Naumov, V., & Gross, T. (2007). Connectivity-aware routing (CAR) in vehicular ad-hoc networks. In *Proceedings of 26th IEEE international conference on computer communications, Infocom 2007*, Anchorage, Alaska, 2007.
31. Leontiadis, I., & Mascolo, C. (2007). GeOpps: geographical opportunistic routing for vehicular networks. In *Proceedings of IEEE international symposium on world of wireless, mobile and multimedia networks (WoWMoM 2007)*, Helsinki, Finland, 2007.
32. Hartenstein, H. (2001). Position-aware ad hoc wireless networks for inter-vehicle communications: the fleetnet project. In *Proceedings of the 2nd ACM international symposium on mobile ad hoc networking & computing*, Long Beach, CA.
33. Blum, J., & Eskandarian, A. (2006). Fast, robust message forwarding for inter-vehicle communication networks. In *Proceedings of IEEE intelligent transportation systems conference (ITSC'06)* (pp. 1418–1423).
34. Yang, K., Ou, S., Chen, H., & He, J. (2007). A multihop peer-communication protocol with fairness guarantee for IEEE 802.16-based vehicular networks. *IEEE Transactions on Vehicular Technology*, *56*(6), 3358–3370.
35. Biswas, S., Tatchikou, R., & Dion, F. (2006). Vehicle-to-vehicle wireless communication protocols for enhancing highway traffic safety. *IEEE Communication Magazine*, *44*(1), 74–82.
36. Chen, Y., Lin, Y., & Lee, S. (2010). A mobicast routing protocol for vehicular ad hoc networks. *ACM/Springer Mobile Networks and Applications*, *15*(1), 20–35.
37. Chen, Y., Lin, Y., & Lee, S. (2010). A mobicast routing protocol with carry-and-forward for vehicular ad hoc networks. In *Proceedings of the fifth international conference on communications and networking in China 2010 (CHINACOM 2010)*, China, Beijing, August 2010.
38. Zhu, J., & Roy, S. (2003). MAC for dedicated short range communications in intelligent transport systems. *IEEE Communications Magazine*, *41*(12), 60–67.
39. Zhao, J., & Cao, G. (2006). *VADD: vehicle-assisted data delivery in vehicular ad hoc networks*. http://mcn.cse.psu.edu/paper/jizhao/infocom06.pdf (accessed: May 29, 2010).
40. Perrig, A. et al. (2002). The TESLA broadcast authentication protocol. *CryptoBytes*, *5*(2), 2–13.
41. Hu, Y.-C., & Laberteaux, K. (2006). *Strong security on a budget, Wksp*. Embedded Security for Cars, Nov. 2006. Also available at www.crhc.uiuc.edu/~yihchun (accessed: May 29, 2010).
42. Hartenstein, H., & Laberteaux, K. (2008). A tutorial survey on vehicular ad hoc networks. *IEEE Communications Magazine*, *June*, 164–171.
43. Raya, M., Papadimitratos, P., & Hubaux, J. (2006). Securing vehicular communications. *IEEE Wireless Communications, Special Issue on Inter-Vehicular Communications*, *13*(5), 8–15.
44. EUROPA (2010). *European road safety charter*. http://ec.europa.eu/transport/roadsafety/charter (accessed: May 29, 2010).
45. IEEE Standard 1609.1-2006 (2006). IEEE trial-use standard for wireless access in vehicular environments (WAVE) (pp. 1–63).
46. IVI (Intelligent Vehicle Initiative) technology—advanced controls and navigation systems. In *Proceedings of society of automotive engineers, SAE world congress*, Detroit, USA, 2005.
47. Shulman, M., & Deering, R. (2007). *Vehicle safety communications in the United States*. US Department of Transportation, National Highway Traffic and Safety Administration (NHTSA). www-nrd.nhtsa.dot.gov/pdf/esv/esv20/07-0010-O.pdf [accessed: May 29, 2010].
48. VII (Vehicle Infrastructure Integration) (2009). *Proof of concept* (Report No. FHWA-JPO-09-003). www.intellidriveusa.org/documents/052009-POC-vehicle-final-report.pdf (accessed: May 29, 2010).
49. Clarion (2010). www.clarion.com/us/en/tech/index.html (accessed: May 29, 2010).
50. www.car-to-car.org (accessed May 29, 2010).
51. Festag, A., Fubler, H., Hartenstein, H., Sarma, A., & Schmitz, R. (2004). FleetNet: bringing car-to-car communication into real world. In *Proceedings of 11th world congress on intelligent transportation systems (ITS'04)*, Nagoya, Japan, October 2004.
52. Hartenstein, H., Fubler, H., Mauve, M., & Franz, W. (2003). Simulation results and a proof of concept implementation of the FleetNet position-based router. In *Proceedings of 8th international conference on personal wireless communications (PWC'03)* (pp. 192–197), Venice, Italy, September 2003.
53. NoW (Network on Wheels) (2008). www.network-on-wheels.de (accessed: May 29, 2010).
54. Schulze, M., et al. (2008). *Integrated projects document 15: final report* (PR-04000-IPD-080222-v16_PReVENT_Final_Report_080507.doc). www.prevent-ip.org (accessed: May 29, 2010).
55. PReVENT (2007). www.prevent-ip.org/en/prevent_subprojects/horizontal_activities/ip_exhibition (accessed: May 29, 2010).
56. CVIS (Cooperative Vehicles and Infrastructure Systems) (2010). www.cvisproject.org (accessed: May 29, 2010).
57. Reichardt, D., et al. (2002). CARTALK 2000 safe and comfortable driving based upon inter-vehicle-communication. In *Proceedings of IEEE intelligent vehicle symposium* (Vol. 2, pp. 17–21), June 2002.
58. Bergese, C., Braun, A., & Porta, E. (1999). Inside CHAUFFEUR. In *Proceedings of 6th ITS world congress*, Toronto, Canada, November 1999.
59. Carlink: Project Consortium (2008). http://carlink.lcc.uma.es/achieve.html (accessed: May 29, 2010).
60. Tsugawa, S., Kato, S., Tokuda, K., Matsui, T., & Fujii, H. (2000). A cooperative driving system with automated vehicles and inter-vehicle communications in Demo 2000. In *Proceedings of IEEE intelligent transportation systems*, Dearborn, MI, 2000.

61. Yasuto, K. (2004). DSRC standards for multiple applications, OKI electric industry. In *Proceedings of 11th world congress on ITS*, Nagoya, Japan, 2004.
62. Wang, J., & Yan, W. (2009). RBM: a role based mobility model for VANET. In *Proceedings of international conference on communications and mobile computing (CMC'09)* (Vol. 2, pp. 437–443), January 2009.
63. Liu, B., Khorashadi, B., Du, H., Ghosal, D., Chuah, C., & Zhang, M. (2009). VGSim: an integrated networking and microscopic vehicular mobility simulation platform—[Topics in automotive networking]. *IEEE Communications Magazine*, *47*(5), 134–141.
64. Fiore, M., Harri, J., Filali, F., & Bonnet, C. (2007). Vehicular mobility simulation for VANETs. In *Proceedings of 40th annual simulation, symposium* (pp. 301–309), March 2007.
65. Tuduce, C., & Gross, T. (2005). A mobility model based on WLAN traces and its validation. In *Proceedings of the IEEE INFOCOM 2005*, Miami, March 2005.
66. Kotz, D., & Henderson, T. (2005). CRAWDAD: a community resource for archiving wireless data at Dartmouth. *IEEE Pervasive Computing*, *4*(4), 12–14.
67. Romano, N., & Numamaker, J. (2001). Meeting analysis: findings from research and practice. In *Proceedings of the 34th Hawaii international conference on systems science*.
68. UDel models for simulation of urban mobile wireless networks (20010). http://udelmodels.eecis.udel.edu/ (accessed: May 29, 2010).
69. Yoon, J., Noble, B., Liu, M., & Kim, M. (2006). Building realistic mobility models from coarse-grained traces. In *Proceedings of the ACM international conference on mobile systems, applications and services (MobiSys'06)* (pp. 177–190).
70. PTV simulation—VISSIM (2010). www.english.ptv.de/cgi-bin/traffic/traf_vissim.pl (accessed: May 29, 2010).
71. CORSIM: microscopic traffic simulation model (2010). http://mctrans.ce.ufl.edu/featured/tsis/Version5/corsim.htm (accessed: May 29, 2010).
72. TRANSIMS (TRansportation ANalysis and SIMulation System) (2010). http://transims.tsasa.lanl.gov (accessed: May 29, 2010).
73. VanetMobiSim project, home page (2010). http://vanet.eurecom.fr (accessed: May 29, 2010).
74. www.census.gov/geo/www/tiger (accessed: May 29, 2010).
75. Sheffer, A., Etzion, M., Rappoport, A., & Bercovier, M. (1999). Hexahedral mesh generation using the embedded Voronoi graph. *Engineering with Computers*, *15*(3), 248–262.
76. Fiore, M. (2006). *Mobility models in inter-vehicle communications literature* (Technical Report). Politecnico di Torino, Italy, November 2006.
77. AIMSUN User Manual, Version 4.1, TSS-Transportation Simulation System, Barcelona, Spain, 2002.
78. VISSIM 3.5 User Manual, PTV Planung Transport Verkehr AG, Germany, 2000.
79. Boxill, S., & Yu, L. (2000). *An evaluation of traffic simulation models for supporting ITS development* (Technical Report 167602-1). Texas Southern University, October 2000.
80. Krauss, S., Wagner, P., & Gawron, C. (1997). Metastable states in a microscopic model of traffic flow. *Physical Review E*, *55*(304), 55–97.
81. Hartenstein, H., et al. (2003). Simulation results and a proof-of-concept implementation of the FleetNet position-based router. In *Proceedings of the eighth international conference on personal wireless communications (PWC'03)* (pp. 192–197), Venice, Italy, September 2003.
82. Karnadi, F., Mo, Z., & Lan, K. (2007). Rapid generation of realistic mobility models for VANET. In *Proceedings of the IEEE wireless communication and networking conference (WCNC'07)* (pp. 2506–2511), Hong Kong, March 2007.
83. Traffic and network simulation environment (2010). http://wiki.epfl.ch/trans (accessed: May 29, 2010).
84. Wang, S., Chou, C., Huang, C., Hwang, C., Yang, Z., Chiou, C., & Lin, C. (2003). The design and implementation of the NCTUns 1.0 network simulator. *Computer Networks*, *42*(2), 175–197.
85. CANU project home page (2010). http://www.ipvs.uni-stuttgart.de/abteilungen/vs/forschung/projekte/Communication_in_Ad-hoc_Networks_for_Ubiquitous_Computing/de (accessed: May 29, 2010).
86. The network simulator ns-2 (2010). http://www.isi.edu/nsnam/ns (accessed: May 29, 2010).
87. Global mobile information systems simulation library. http://pcl.cs.ucla.edu/projects/glomosim (accessed: May 29, 2010).
88. http://sumo.sourceforge.net (accessed: May 29, 2010).
89. Wang, S., & Chih-Che, L. (2008). NCTUns 5.0: a network simulator for IEEE 802.11(p) and 1609 wireless vehicular network researches. In *Proceedings of IEEE 68th vehicular technology conference (VTC Fall 2008)*, Calgary, Canada, September 2008.
90. Harri, J., Filali, F., & Bonnet, C. (2007). *Mobility models for vehicular ad hoc networks: a survey and taxonomy* (Technical Report RR-06-168). Department of Mobile Communications, Institut Eurecom, France, March 2007.
91. Sun, S., Kim, J., Jung, Y., & Kim, K. (2009). Zone-based greedy perimeter stateless routing for VANET. In *Proceedings of international conference on information networking (ICOIN 2009)* (pp. 1–3), January 2009.
92. Luo, P., Huang, H., Shu, W., Li, M., & Wu, M. (2008). Performance evaluation of vehicular dtn routing under realistic mobility models. In *Proceedings of IEEE wireless communications and networking conference 2008* (pp. 2206–2211), April 2008.
93. Chung, S.-E., Yoo, J., & Kim, C.-K. (2009). A cognitive MAC for VANET based on the WAVE systems. In *Proceedings of 11th international conference on advanced communication technology (ICACT 2009)* (Vol. 1, pp. 41–46), February 2009.
94. Ali, S., & Bilal, S. (2009). An intelligent routing protocol for VANETs in city environments. In *Proceedings of 2nd international conference on computer, control and communication (IC4 2009)*, Karachi, Pakistan, February 2009.
95. Okada, H., Takano, A., & Mase, K. (2009). A proposal of link metric for next-hop forwarding methods in vehicular ad hoc networks. In *Proceedings of 6th IEEE consumer communications and networking conference 2009, CCNC 2009*, Las Vegas, January 2009.
96. Jerbi, M., Senouci, S.-M., Meraihi, R., & Ghamri-Doudane, Y. (2007). An improved vehicular ad hoc routing protocol for city environments. In *Proceedings of IEEE international conference on communication (ICC 2007)* (pp. 3972–3979), Glasgow, Scotland.
97. Verma, M., & Dijiang, H. (2009). SeGCom: secure group communication in VANETs. In *Proceedings of 6th IEEE consumer communications and networking conference 2009, CCNC 2009*, Las Vegas, January 2009.
98. Choi, J., & Jung, S. (2009). A security framework with strong non-repudiation and privacy in VANETs. In *Proceedings of 6th IEEE consumer communications and networking conference 2009, CCNC 2009*, Las Vegas, January 2009.
99. Wiegel, B., Gunter, Y., & Grossmann, H. (2009). A concept on signalling spacial network conditions to provide quality of service in a VANET. In *Proceedings 2nd international conference on signal processing and communication systems (ICSPCS 2008)* (pp. 1–10), December 2008.
100. Boban, M., Misek, G., & Tonguz, O. (2008). What is the best achievable QoS for unicast routing in VANETs? In *Proceedings of IEEE GLOBECOM workshops* (pp. 1–10), December 2008.
101. Ramirez, C., & Veiga, M. (2007). QoS in vehicular and intelligent transport networks using multipath routing. In *Proceedings of IEEE international symposium on industrial electronics (ISIE 2007)* (pp. 2556–2561), June 2007.

102. Ciccarese, G., De Blasi, M., Marra, P., Palazzo, C., & Patrono, L. (2009). On the use of control packets for intelligent flooding in VANETs. In *Proceedings of IEEE wireless communications and networking conference (WCNC 2009)* (pp. 1–6), April 2009.
103. Amoroso, A., Roccetti, M., Nanni, M., & Prati, L. (2009). VANETS without limitations: an optimal distributed algorithm for multi-hop communications. In *Proceedings of 6th IEEE consumer communications and networking conference 2009, CCNC 2009*, Las Vegas, January 2009.
104. Yang, L., Guo, J., & Wu, Y. (2009). Piggyback cooperative repetition for reliable broadcasting of safety messages in VANETs. In *Proceedings of 6th IEEE consumer communications and networking conference 2009, CCNC 2009*, Las Vegas, January 2009.

Sherali Zeadally received his Bachelor's Degree in Computer Science from University of Cambridge, England, and the Doctoral Degree in Computer Science from University of Buckingham, England in 1996. He is an Associate Professor at the University of the District of Columbia. He currently serves on the Editorial Boards of over 15 peer-reviewed international journals. He has been serving as a Co-Guest editor for over a dozen special issues of international scholarly journals in the areas of networking. He is a Fellow of the British Computer Society and a Fellow of the Institution of Engineering Technology, UK. His research interests include computer networks including wired and wireless networks), network and system security, mobile computing, ubiquitous computing, RFID, performance evaluation of systems and networks.

Ray Hunt is an Associate Professor specializing in Networks and Security in the College of Engineering at the University of Canterbury, Christchurch, New Zealand. His areas of teaching and research are networks, security and forensics He heads the Computer Security and Forensics Post Graduate Diploma program at the University of Canterbury.

Yuh-Shyan Chen received the Ph.D. degrees in Computer Science and Information Engineering from the National Central University, Taiwan, ROC., in January 1996. He now has been a Professor at the Department of Computer Science and Information Engineering, National Taipei University, Taiwan. Prof. Chen served as Editor-in-Chief of International Journal of Ad Hoc and Ubiquitous Computing (SCIE), Regional Editor (Asia and Pacific) of IET Communications (SCI), Editorial Board of Telecommunication System Journal (SCIE), EURASIP Journal on Wireless Communications and Networking (SCIE), International Journal of Communication Systems (SCIE), and Mobile Information Systems (SCIE). Dr. Chen is a senior member of the IEEE Communication Society.

Angela Irwin is a graduate of the University of Canterbury in New Zealand. She is currently a PhD student in the School of Computer and Information Science at the University of South Australia researching on Money Laundering and Terrorism Financing in Virtual Environments. Her areas of interests include computer forensics, money laundering detection methods, techniques and behavior modeling.

Aamir Hassan holds a bachelor's degree in Computer Science from the University of Peshawar, Pakistan. He holds various CISCO certifications in networking and security. He also has a Master's degree in Computer Network Engineering from the Halmstad University, Sweden.