Computer Communications 33 (2010) 775–793

Contents lists available at ScienceDirect

Computer Communications

journal homepage: www.elsevier.com/locate/comcom

Vehicular telematics over heterogeneous wireless networks: A survey

Ekram Hossain [a], Garland Chow [b], Victor C.M. Leung [c,*], Robert D. McLeod [a], Jelena Mišić [d], Vincent W.S. Wong [c], Oliver Yang [e]

[a] Department of Electrical and Computer Engineering, University of Manitoba, Winnipeg, Canada
[b] Sauder School of Business, University of British Columbia, Vancouver, Canada
[c] Department of Electrical and Computer Engineering, University of British Columbia, Vancouver, Canada
[d] Department of Computer Science, Ryerson University, Toronto, Canada
[e] School of Information Technology and Engineering, University of Ottawa, Canada

ARTICLE INFO

Article history:
Received 19 May 2009
Received in revised form 16 December 2009
Accepted 24 December 2009
Available online 7 January 2010

Keywords:
Intelligent transportation systems
Vehicular telematics
Heterogeneous wireless networks

ABSTRACT

This article presents a survey on vehicular telematics over heterogeneous wireless networks. An advanced heterogeneous vehicular network (AHVN) architecture is outlined which uses multiple access technologies and multiple radios in a collaborative manner. The challenges in designing the essential functional components of AHVN and the corresponding protocols (for radio link control, routing, congestion control, security and privacy, and application development) are discussed and the related work in the literature are reviewed. The open research challenges and several avenues for future research on vehicular telematics over heterogeneous wireless access networks are outlined.

1. Introduction

Vehicular telematics and infotainment applications will be key to developing Intelligent Transportation Systems (ITS) in order to achieve safety and productivity in transportation. Wireless communications and networking technologies such as IEEE 802.11 (WiFi), IEEE 802.16 (WiMAX), 3G cellular, and satellite technologies will be vital to support data communications for vehicular telematics. The ITS America VII (Vehicle-Infrastructure Integration) framework proposed wireless communications in the 5.9 GHz band for automotive use [1] and the US Department of Transportation (DoT) proposed a system architecture for development of ITS [2].

ITS applications can be supported through vehicle-to-roadside (V2R) and vehicle-to-vehicle (V2V) communications. V2R communications involve vehicular nodes and road side base stations. IEEE 802.11 (WiFi) [3], IEEE 802.16 (WiMAX) [5], and Dedicated Short Range Communications (DSRC) [6] technologies can be used in this model of communication. In particular, with the DSRC standard, onboard units (OBUs) placed at each vehicle can send or receive data to or from roadside units (RSUs). However, if a vehicle cannot directly send its data to an RSU, it can relay its data to other vehicles until the data reach the RSU using a multihop transmission strategy [7]. It is also possible that OBUs form a group and elect the group leader. In this case, all group member OBUs will send their reports to the leader OBU which will aggregate them and forward the resulting message(s) to the RSU. There are several applications for this communication model such as electronic toll collection, infotainment services, safety message dissemination, and web browsing. Besides the on-board computer and communication interface, OBUs are typically equipped with a Global Positioning System (GPS), which provides information on vehicle position in real-time, and an event data recorder, which stores relevant data that, in case of an accident, can be used in forensic analysis. RSUs act as base stations or access points, and are connected to application servers. RSUs and servers can be run by the Department of Transportation (federal, provincial, or local), Police Department, or third party providers.

V2V communications involve vehicular nodes on a road which form a vehicular ad hoc network (VANET). This mode of communication is mainly used in safety warning system [2,8], traffic information system [9], and multimedia streaming [10]. Collision avoidance, road obstacle warning, intersection collision warning, and lane change assistance are example applications of V2V communications. Most of V2V safety applications require low transfer latency since these applications are used in a dynamic and unpredictable traffic environment. Most of researches tend to find

* Corresponding author. Address: Department of Electrical and Computer Engineering, University of British Columbia, Room 4013, Kaiser Building, 2332 Main Mall, Vancouver, BC, Canada V6T 1Z4. Tel.: +1 604 822 6932; fax: +1 604 822 5949.
E-mail addresses: ekram@ee.umanitoba.ca (E. Hossain), Garland.Chow@sauder.ubc.ca (G. Chow), vleung@ece.ubc.ca (V.C.M. Leung), mcleod@ee.umanitoba.ca (R.D. McLeod), jmisic@cs.umanitoba.ca (J. Mišić), vincentw@ece.ubc.ca (V.W.S. Wong), yang@site.uottawa.ca (O. Yang).

0140-3664/$ - see front matter © 2010 Elsevier B.V. All rights reserved.
doi:10.1016/j.comcom.2009.12.010

improvements of such medium access control (MAC) protocols, transmission strategies, and wireless technologies in order to reduce the latency.

By definition, emerging vehicular telematic applications will be wireless. In the past, there has been an emphasis on providing wireless services to individuals, such that they may make alternative route decisions in a more or less independent manner. These are essentially first generation applications where the users are autonomous and assumed independent, such as simple direction systems based on GPS. The conceptual objective of these first-generation applications is to define or identify, and then to reproduce or represent a measured parameter (e.g., location) back to the user. Without doubt many have envisioned the day, when at the end of the month a bill will arrive with several GPS/accelerometer detected infractions, parking, speeding, dangerous driving, non-compliant engine off etc. combined with a micro-bill for each transgression. Early vehicular telematic applications were/are user-centric as well as the latter seemingly coming from a "brave new world".

This article provides a survey on the research issues, challenges, and possible approaches to tackle these challenges for vehicular telematics over heterogeneous wireless networks. This survey includes the concepts considered and analyzed in existing collections of papers obtained as the outcome of some recent and ongoing research projects [11–20]. A survey of the related projects carried out in Europe, USA, and Japan can be found in [23]. Based on the publicly available information, in this survey, the authors summarized the scope and application type of 79 projects that included wireless vehicle-to-infrastructure and vehicle-to-vehicle communications. It was observed that there are higher number of projects in Europe as compared to USA and Japan. However, there are more overlapping projects (i.e., addressing the same issues) in Europe as compared to USA and Japan. While the projects in Europe and USA focus mainly on safety applications, the projects in Japan primarily focus on vehicular traffic congestion applications. It was also observed that the USA and European projects end with a demonstrator or theoretical results, while the Japanese projects end with a product and deployment.

The outline of the rest of the article is as follows. Section 2 describes different types of vehicular telematic applications and their requirements. The advanced heterogeneous vehicular network (AHVN) architecture is presented in Section 3. Sections 4, 5 discuss the challenges and approaches in designing the functional components and protocols for AHVN. Finally, the open research issues and several directions for future research related to vehicular telematics over AHVN are outlined in Section 6.

2. Vehicular telematic applications and requirements

Three general types of applications are anticipated to be developed over vehicular networks. Safety applications are the first type of applications that improve the safety of the passengers on the roads by notifying the vehicles about any dangerous situation in their neighbourhood. Well-known examples are collision warnings such as notifications about a chain car accident, warnings about road conditions such as slippery road, approaching emergency vehicle warning, etc. The main concern here is finding low-latency, reliable, and efficient methods for disseminating safety data among neighbouring vehicles. A large number of data dissemination mechanisms were proposed in the literature. While many of these works rely on repeaters and (or) access points (APs) for disseminating the safety data [24,25], some other works suggest that infrastructure-independent fully ad-hoc communications suffice [26,27].

Another type of applications is traffic applications that call for the deployment of Traffic Information Systems (TISs), which carry out traffic management and provide drivers with the traffic situation and road information. The drivers use this information to avoid congestion and to find the route with minimum delay to their destinations. In other words, TISs aim at balancing the vehicular traffic on streets in order to use the capacity of streets and junctions efficiently and consequently save the lives and reduce the travel time and waste of energy. One of the seminal TISs is self-organizing traffic information system (SOTIS) [28], in which each road is divided into several segments, and vehicles send the average velocities of the segments periodically. TrafficView [29] is another TIS which has a mechanism similar to SOTIS, but instead of the average velocities in the segments, it disseminates the positions and velocities of the individual vehicles periodically. The authors of SOTIS expanded the idea of SOTIS to develop a segment-oriented data abstraction and dissemination (SODAD) scheme in their more recent work [30] which has an adaptive approach. All these studies, however, are fully ad-hoc TISs and suffer from large delays at far distances and not having a reliable mechanism to make sure that every vehicle is provided with all the traffic information it needs. The coexistence of infrastructure-based and ad-hoc wireless communications, i.e., a wireless mesh type of architecture could overcome these problems. One of the substantial challenges that should be addressed in traffic applications is the data aggregation algorithm the TIS employs to include as much traffic information as possible in the traffic packets vehicles broadcast. Different data aggregation algorithms in the literature will be described later in this article.

The third type of vehicular applications is non-safety applications also called comfort or entertainment applications. Non-safety applications are so varied, ranging from real-time or non real-time multimedia streaming and interactive communications such as video-conferencing and interactive games to roadside service application such as location and price lists of restaurants or gas-stations, weather information or Internet access such as data transfer, web browsing, music download and etc. Note that multimedia streaming is used for a wide range of applications. Even in traffic or safety applications the traffic situation or emergency message can be generated by video sensors already installed along the roadside.

In contrary to the first-generation vehicular telematic applications, the emerging generation of wireless applications capitalize on the extraction of data from fleets of multiple vehicles. Data mining on the extracted data can aid better decision support of difficult-to-predict emergent behavior. The conceptual objective of these second-generation applications is to translate or convert multi-source data, and then to estimate or infer extant conditions back to the users as well as interested third parties. Examples of this include highway safety systems where wireless intra-vehicle relays can be used to impede or halt oncoming traffic in a freeway accident scenario (forward collision warning). These are somewhat obvious applications that are built upon layers of sophisticated technology with vehicle safety systems leading the development.

In addition, there is a class of applications that rely on inference from probes or floating cars, with the intent is to capture a statistically significant portion of vehicle behavior such that meaningful inferences can be made and potentially generalized to the entire population of vehicles [31]. Applications include infrastructure monitoring as well as sampling empirical data input for traffic flow control. In the infrastructure health monitoring application (Fig. 1), fleet of vehicles such as busses would incorporate additional sensors to those routinely on-board. An instance may be monitored sacrificial anodes, accelerometers or strain gauges coupled to GPS etc. that would collect data to provide information on the structural integrity of the vehicle on various routes as well as for various drivers. An instance of emission factor estimation (Fig. 2) can be one similar in architecture to the infrastructure health monitoring application albeit enhanced through reliance on statistical sam-

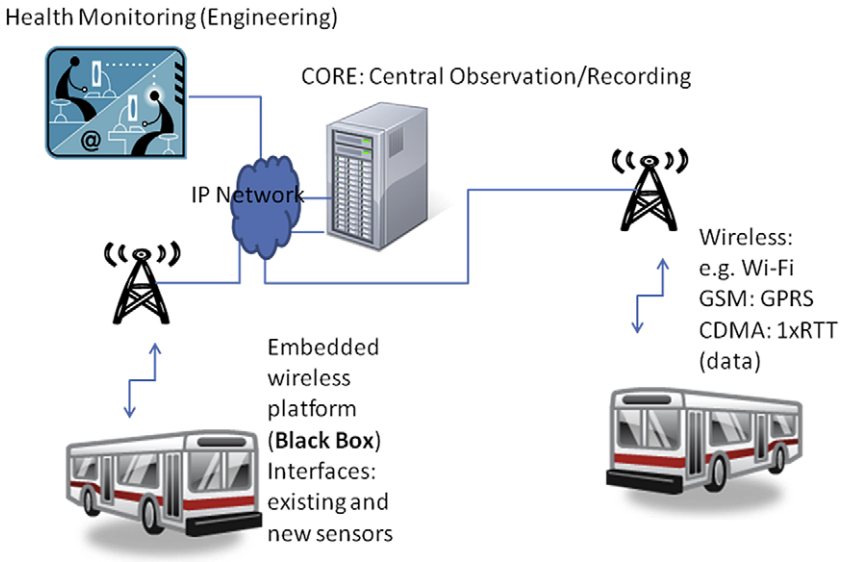


Fig. 1. Infrastructure health monitoring.

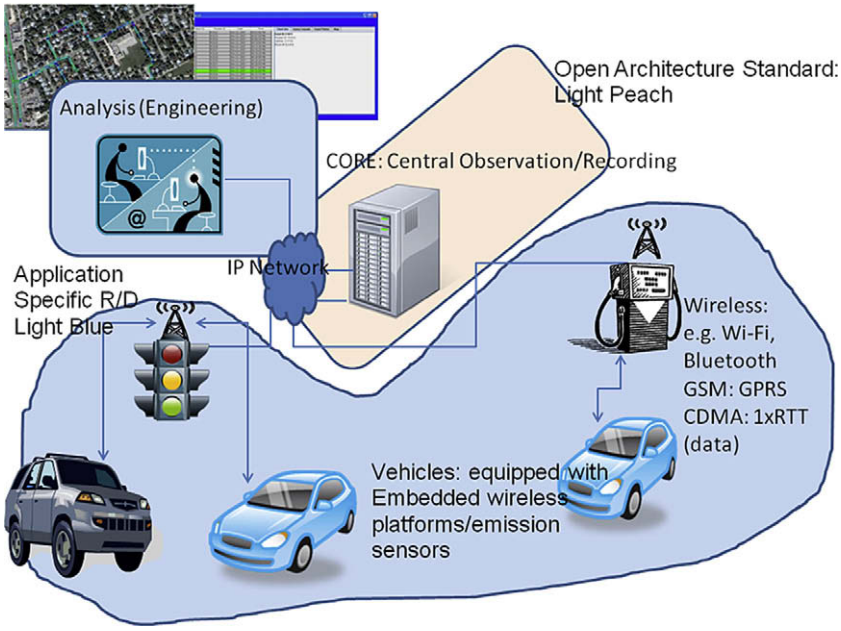


Fig. 2. An emission factor statistical estimation architecture.

pling. In some cases, only a very small amount of floating car data is required to infer significant event such as congestion build-up or dissolution [32]. These newer applications are more cohort-centric as opposed to being individual or user-centric. In these latter cases data needs to be backhauled (wirelessly) and processed centrally, as it would be impractical to have all probe data processed onboard each probe vehicle. As such, this type of requirement mandates the use of data collection management, operating system and application management systems. Relevant data can then be sent to information sinks (probes as well as third parties) informing them of road or condition hazards, for example. Because not all information broadcast would be useful to all recipients, filtering applications will have to be developed that provide the operator with useful information. For example, if a statistically significant percentage of probes detect a road hazard after central processing, only vehicles in the local (context-specific) area would need to be informed (local area being context specific).

3. Advanced Heterogeneous Vehicular Network (AHVN) architecture for vehicular telematics

Most of the studies in the field of vehicular communications and vehicular networks only deal with a single type of application in these networks, i.e., none of them addresses all types of safety, traffic and comfort applications, and neither purely infrastructure-based or purely ad-hoc vehicular networks nor even traditional single radio wireless mesh networks meet the requirements of all the applications at the same time. We believe that an advanced heterogeneous vehicular network (AHVN) that uses multiple radios and multiple access technologies in a collaborative manner could be the best candidate for a vehicular network.

A key motivation of considering the AHVN is that DRSC will only be effective when it is ubiquitously deployed, but this will not happen until the needed infrastructure is in place, governments legislate for DSRC deployment in passenger vehicles, and older non-

compliant vehicles have retired. This is not very likely to happen within the next 10–20 years. Therefore, in the meantime a heterogeneous platform is the best way forward. In fact, on the issue of infrastructure deployment, the ITS branch of the US DoT is still exploring different business models, as it is not certain that public sector can or wish to cover all the costs.

The access technologies that can be employed as well as the architecture of AHVN including the functional components and their logical relations along with the challenges that should be addressed are discussed in this section.

3.1. The access technology options

In the AHVN, the vehicles request services with different requirements in terms of latency, bandwidth, error rate, area of coverage, etc. at any time and any place. Existing access technologies such as wireless LANs (WLAN IEEE 802.11a/b/g/n/p standards), WiMAX (IEEE 802.16 a/e standards), ultra wideband (UWB IEEE 802.15.3a standard), third and fourth generation cellular wireless (3G and 4G), satellite communications etc. are designed for specific service requirements.

- *IEEE 802.11*-based WLAN which has achieved a great acceptance in the market supports short-range relatively high-speed data transmission. The maximum achievable data rate in its latest version 802.11n is about 100 Mbps. Although some studies have shown its performance reduction due to interference [33], the viability of its deployment for the nodes moving at vehicular speeds has already been confirmed in several papers [34–37]. On the other hand, the short transmission range leads to frequent transmission interruption particularly when vehicle speed is high and consequently many access points have to be deployed along the road that incurs high deployment cost [38,39].
- IEEE 802.11p is a new communication standard in the IEEE 802.11 family which is based on the IEEE 802.11a. IEEE 802.11p, which is also referred to as the DSRC standard, is designed for wireless access in the vehicular environment (WAVE) [8,3,6] to support ITS applications. For DSRC, 75 MHz of licensed spectrum at 5.9 GHz has been allocated which consists of 7 channels (10 MHz each) for supporting safety and non-safety applications.DSRC supports a very high data rate (6–27 Mbps) with a maximum communication range of 1000 m. Presently DSRC is mainly used in electronic toll collection. Potential applications of DSRC are: emergency warning systems for vehicles, adaptive cruise control, forward collision warning, electronic parking payments, approaching emergency vehicle warning, transit or emergency vehicle signal priority, and in-vehicle signing. Vehicles equipped with DSRC can communicate directly with each other, making it possible to send warning messages to neighboring vehicles. DSRC can also be used to provide in-vehicle entertainment for drivers and passengers.
- *IEEE 802.16* standard-based WiMAX (Worldwide Interoperability for Microwave Access) systems are able to cover a large geographical area, up to 50 km, and to deliver significant bandwidth to end-users up to 72 Mbps theoretically. While IEEE 802.16 standard only supports fixed broadband wireless communications, IEEE 802.16e/mobile WiMAX standard supports speeds up to 160 km/h and different classes of quality of service, even for non-line-of-sight transmissions. In WLAN, a contention-based channel access mechanism is used which can cause subscriber stations distant from the AP to be repeatedly interrupted by closer stations. The key advantage of WiMAX compared to WLAN is that the channel access method in WiMAX uses a scheduling algorithm for which the subscriber station needs to compete only once for initial entry into the network. After that, it is allocated an access slot by the BS. Table 1 shows a list of some applications envisioned by mobile WiMAX and their QoS requirements [5].
- For vehicular telematic services, *3G cellular wireless* technology can provide a very broad coverage and support high-mobility vehicles [40]. Current 3G networks deliver a data rate of 384 kbps to moving vehicles which goes up to 2 Mbps for fixed nodes. 3G systems deliver smoother handoffs compared to WLAN and WiMAX systems, however, due to centralized switching at mobile switching centre (MSC) or serving GPRS support node (SGSN), their latency may become an issue for many appli-

Table 1
Mobile WiMAX application and quality of service.

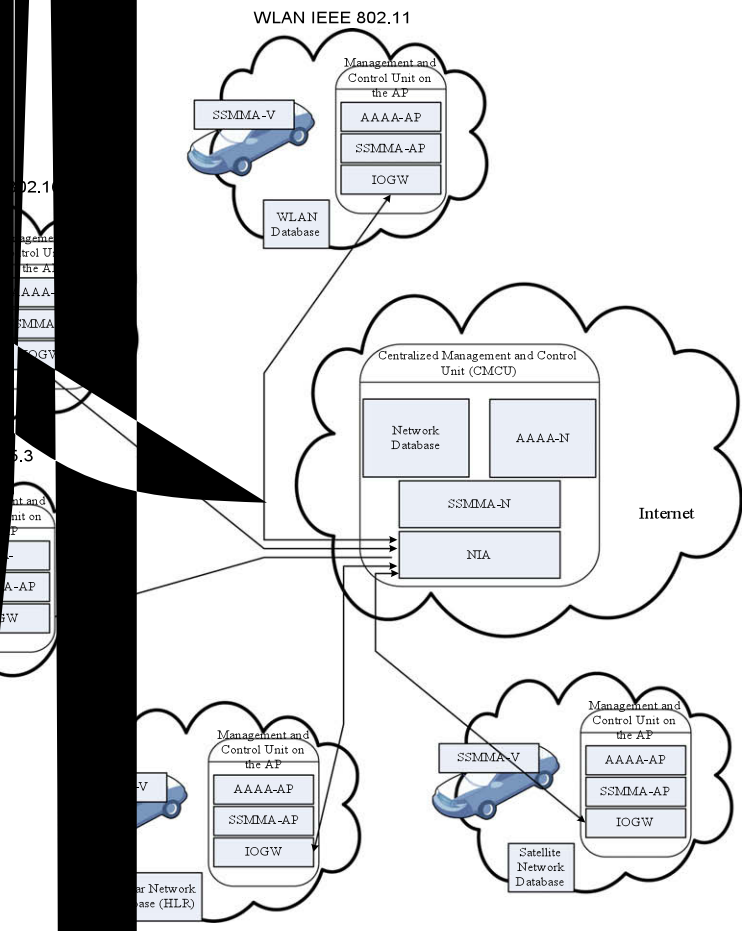
QoS Category	Applications	QoS Specifications
UGS Unsolicited Grant Service	VoIP	• Maximum Sustained Rate • Maximum Latency Tolerance • Jitter Tolerance
rtPS Real-Time Polling Service	Streaming Audio or Video	• Minimum Reserved Rate • Maximum Sustained Rate • Maximum Latency Tolerance • Traffic Priority
ErtPS Extended Real-Time Polling Service	Voice with Activity Detection (VoIP)	• Minimum Reserved Rate • Maximum Sustained Rate • Maximum Latency Tolerance • Jitter Tolerance • Traffic Priority
nrtPS Non-Real-Time Polling Service	File Transfer Protocol (FTP)	• Minimum Reserved Rate • Maximum Sustained Rate • Traffic Priority
BE Best-Effort Service	Data Transfer, Web Browsing, etc.	• Maximum Sustained Rate • Traffic Priority

access in which the ad-hoc communications among vehicles are via IEEE 802.16 air-interface cards. The authors in [45] focused on IEEE 802.16e access technology, and integrated it with ad-hoc communications to introduce a mobility pattern-aware routing protocol for vehicular networks by equipping the vehicles with both IEEE 802.11 and IEEE 802.16 wireless interfaces. None of these studies, however, satisfies all the required services and applications outlined earlier. On the other hand, with the decreasing cost of wireless transceivers, more radios, i.e., more than one radio, can be used in the OBU of a vehicle which forms a heterogeneous architecture rather than simple single radio WMNs. Cooperative use of the multiple radios enhances the performance of the network in the sense that the capacity of the network is improved by allowing more parallel transmissions in different frequencies.

3.2. The essential functional components and their logical relations

A simplified architecture for the AHVN is shown in Fig. 3 with its functional components, and their interactions.

- The Centralized Management and Control Unit (CMCU) is the entity in the core network that contains all the building blocks described below.
- Inter-operating third party agent [46]: The AHVN is composed of heterogeneous wireless systems, each with a different service provider. Since direct service level agreements (SLAs) among different providers are not feasible, [22] proposed the use of a third party agent and every individual service provider only estab-



lishes a direct SLA with the third party agent. The third party agent is commonly referred to as network inter-operating agent (NIA).

- We propose Mobile IPv6 [47] as the interconnecting protocol for integrating various access technologies, which ensures a cost-efficient and scalable core backhaul network and keeps the transparency to the underlying access technologies. Moreover, switching from one access network to another could be mapped into roaming from one wireless network to another, and could be easily addressed considering that a Care-of-Address (CoA) is assigned to each of the vehicles' radios (i.e., one single IP multi-homed over different radios). WiMAX, WiFi, DSRC, and 3G-LTE technologies are expected to have support for IPv6.
- The system (or network) selection and mobility management agent (SSMMA): Selecting the most appropriate access network, implementing mobile IP functionalities using home agent (HA) and foreign agent (FA) concepts, and seamless switching among different networks which is referred to as vertical or intersystem handoff are among the tasks of SSMMA and can be implemented by employing different mechanisms. In other words, this agent intelligently integrates heterogeneous access networks, each of which is optimized for specific service requirements, in a cooperative manner to provide "always best connection (ABC)" to the vehicles.
- Inter-operability gateways (IOGW): In addition to interconnecting the access network to the Internet as a lower layer task, it also takes care of higher layer tasks ranging from establishment of the direct SLA with the NIA to managing interactive conversations with the SSMMA and sharing user profile databases with the SSMMA. Note that access networks with different service providers use separate gateways even if they are providing the same access technology.
- The position and status of the vehicles, the neighboring information, the access radio type that the vehicles are equipped with as well as all the wireless link states in the communication area and the characteristics of roads all should be considered for system selection and mobility management functionalities. This information could be extracted from the databases of the access networks which have SLAs with the NIA, e.g., home location register (HLR) in cellular network, etc. and should be shared among the entities in the AHVN that are in charge of radio management and control responsibilities. On the core network side, all the information of this type could be stored in a network database.
- The AHVN also needs to have an authentication, authorization, accounting, and auditing agent (AAAA) which supports security and billing issues in the network. This functionality could also be distributed over the different access networks due to the different billing and authentication methods used the different service providers.

4. Designing the AHVN architecture: challenges and approaches

4.1. Selection of access network

This functionality could be accomplished by the vehicle, AP or the CMCU in the core network. In the vehicle-based system selection, the vehicles collect all the data they could obtain in their neighboring area and select the radio with the lowest cost that also satisfies their required QoS. This non-centralized mechanism, however, is sub-optimal due to the vehicles limited access to the global network status information. The system selection could also be carried out by the APs of the access network the vehicles have registered in as their home agents (HAs) or by the CMCU. As the system selection responsibility goes towards the core network, the system selection procedure becomes more centralized and more globally optimal. However, the computing and traffic burden is mostly transferred to the CMCU which in addition to incurring high costs for service providers as well as vehicles, might not be appropriate for all applications. For example, the communication though the CMCU instead of direct communication and high traffic load in the CMCU might incur non-tolerable delays in safety applications. Moreover, the vehicles' system preferences are also not taken into consideration. Therefore, we believe that a combination of the above approaches, i.e., breaking down the SSMMA into several SSMMAs on the sides of both vehicles and core network, i.e., SSMMA-V (on the vehicle side) and SSMMA-N (on the network side) could be a good candidate. SSMMA-V and SSMMA-N have a master-slave type of interaction in order to finally select the interface that in spite of satisfying the service requirements incurs the least cost and least interference.

In the access network selection process, the vehicles' highest priority is to activate the interface with lowest price that satisfies its service requirements. However, the network selection process should also consider traffic load balancing, the least interference to other users and consequently the most efficient resource utilization in the network which in turn maximize its revenue. Therefore, some compromising mechanism should be employed to keep both vehicles and service providers satisfied. Some relevant studies were conducted in [33,48], and [49].

Note that in the network selection procedure, the application for which the interface is being chosen plays an important role. As an example, consider a scenario in which an emergency situation is detected by an 802.16 radio-equipped vehicle. Since not all the vehicles in the neighboring area are equipped with 802.16 radios, the AHVN should make other access networks in the area send notifications as well to ensure that every vehicle in the danger area becomes aware of the emergency situation.

4.2. Network selection Vs. link selection Vs. inter-system handoff

Whether to employ the same access technology over all the links in an end-to-end route over multiple hops, or to employ the most appropriate access interface in every hop, which might incur a considerable cost of inter-system handoff, latency and traffic load, is still an open problem. On the other hand, for some applications it might even be more efficient, in terms of handoff cost and complexity to select the access technology only once when the service is initially admitted to the system, although in this case, any failure during the service time initiates the system selection process again.

In the AHVN, resource management in multiple access networks should be addressed in order to maximize the resource utilization, robustness and stability of the network. Although still an open problem, some approaches could be the use of efficient system selection and handoff mechanisms along with dynamic spectrum sharing through software-defined radios. A game-theoretic approach was used in [50] for network selection in a heterogeneous wireless access scenario which ensures fairness among the users. A utility-based network selection scheme was proposed in [51]. An auction-based resource allocation method for heterogeneous wireless access was presented in [52]. The problem of seamless roaming and handoff across cellular networks and WLANs was addressed in [53,54].

4.3. Hierarchical design

In order to guarantee the scalability of the AHVN, a hierarchical structure could be considered for network components such as the NIA [46], the SSMMA, the network database, etc. in which components of the regional level, i.e., first-tier components, are integrated to form the second-tire components and the integration process

continues until the whole network is covered. Determining the number of tiers and the number of elements per tier could itself be an open problem.

4.4. Operating system and application management

For vehicular telematic applications which are collaborative in nature, it is important that the underlying software infrastructure supports multiple mobile platforms in a ubiquitous manner. When applications are developed or modified, they need to be automatically uploaded to the probes, similarly when operating system patches are required; the update has to be seamless without the requirement of individual operator intervention. Without considerable forethought into these issues, the systems being developed extempore will not scale. This issue was investigated and a first generation remotely managed operating system (OS) and application server was prototyped in [55]. It was observed that these systems are complex enough to warrant high level abstractions and implementations are identical to those developed under the auspices of Services Oriented Architectures (SOA) and web services [56]. In addition, there is a need for an open architecture standard to be developed to relieve the application developers of the details of supporting layers in the protocol stack.

5. Designing the AHVN protocols: challenges and approaches

In this section, we discuss the major challenges in protocol design for vehicular networks and the recent research activities corresponding to these challenges.

5.1. Wireless access strategies

Fig. 4 illustrates the major components of the networking model for vehicular telematics. This model consists of the basic functionalities necessary for data communications and the vehicular telematic applications. The communication model can be designed and optimized to support specific applications.

Transmission strategies determine how data packets are delivered from a vehicular node to an RSU (and vice versa) or from a vehicular node to another vehicular node. A *direct transmission* or *single hop* transmission strategy (e.g., in Fig. 5) can be used where

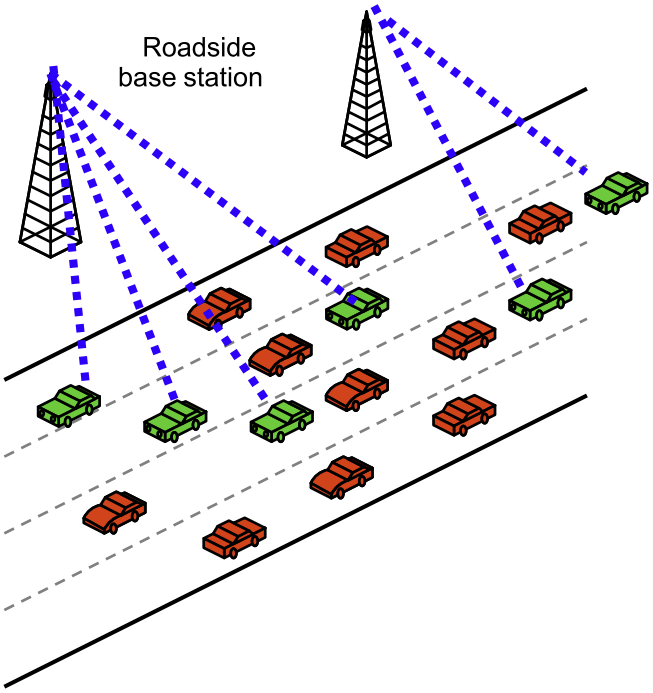


Fig. 5. A model of direct transmission in V2R networks.

an RSU or a vehicular node can be reached directly from a vehicular node (e.g., [40,57,58]). If an RSU or a vehicular node is located far away from a source node, a *multihop* transmission strategy can be employed (e.g., in Fig. 7). In this scenario [42,59], data packets from a vehicular node are relayed by other vehicular nodes until they reach the destination (e.g., coordinated external peer communications (CEPEC) in [7]). Finally, a *cluster-based* transmission strategy forms groups (i.e., clusters) of vehicles, selects a representative (i.e., a cluster head or a gateway) for each group, and transmits data through the selected representative (e.g., in Fig. 6). The cluster head receives data packets from its cluster members and then relay the packets to the RSU (and vice versa). This strategy is efficient to decrease request/data congestion at the RSUs [60].

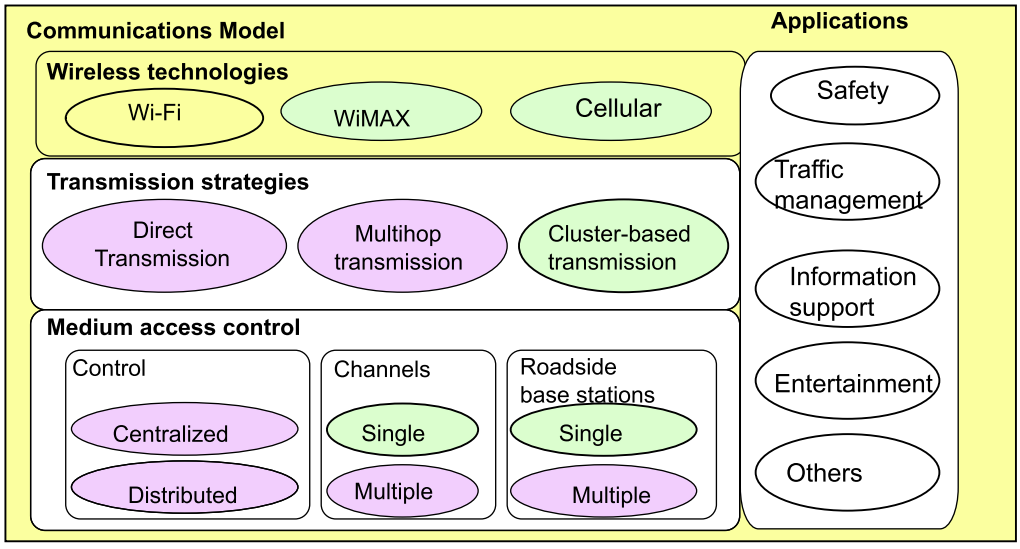


Fig. 4. Wireless access strategies in AHVN.

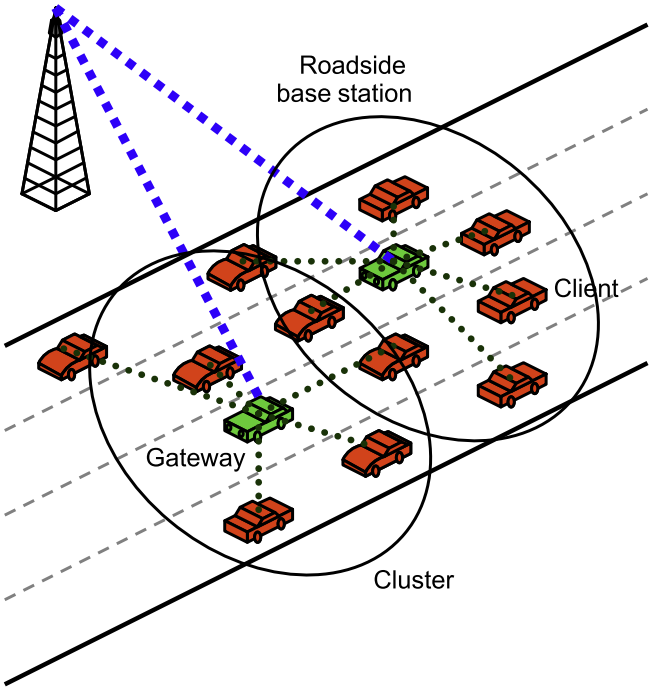


Fig. 6. A model of cluster-based transmission in V2R networks.

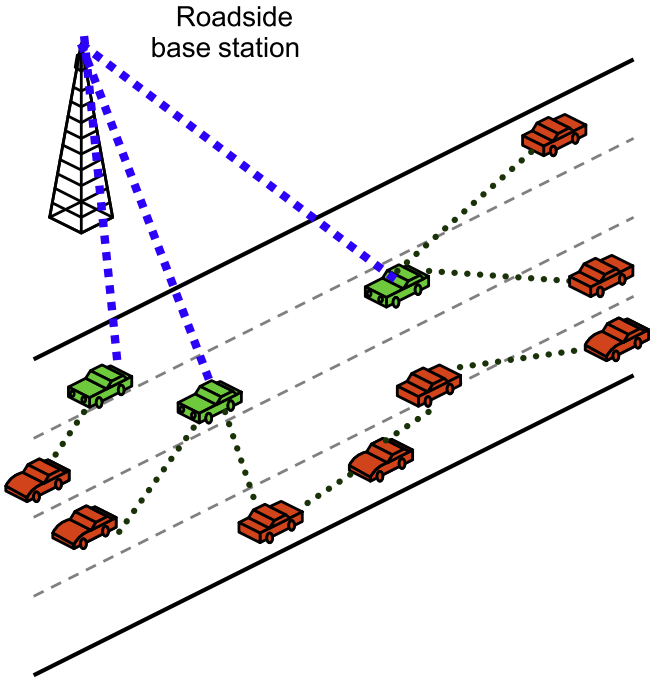


Fig. 7. A model of multihop transmission in V2R networks.

In [7], a cluster-based multihop transmission model was presented. Vehicles on a road, which is divided into equal segments, are grouped into several clusters. Which cluster a vehicle will join depends on its position of the road. For each cluster, a cluster head is chosen based on two criteria: a cluster head must be within a segment border for a segment's life cycle and it must be the vehicle which is closest to the centre of its segment. The cluster members transfer their data to the corresponding cluster head which acts as a gateway. The data packets are merged into a new packet and the cluster head relays the new data packet to other cluster heads until

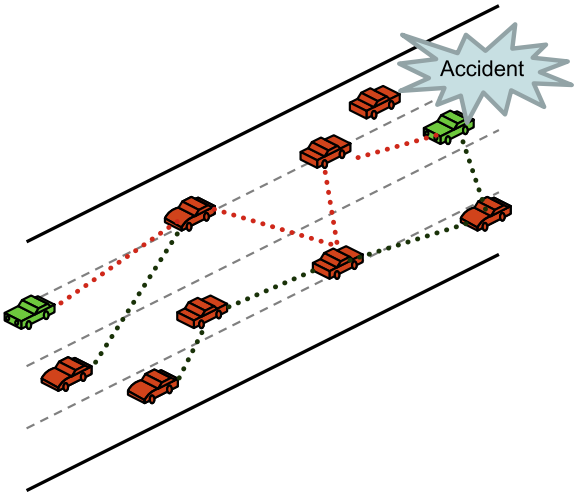


Fig. 8. A model of multihop transmission in V2V networks.

the data reaches the RSU. To guarantee transmission fairness, the RSU assigns an equal amount of bandwidth to each road segment. A multihop V2R communication model and a method based on proxy cache for efficient data access from the Internet were presented in [42].

In [40], a one-hop V2V transmission model was used for disseminating travel and traffic information in vehicular networks. A vehicle acts like a moving wireless station which sends travel and traffic information available at its location to other vehicles on the road. Other vehicles can determine whether the received information is up-to-date or not by using the time stamp information.

For V2V communications, multihop broadcast scheme is used when a target vehicle is out of the transmission range of a broadcasting vehicle. In vehicular safety applications, this transmission strategy is used to transmit warning messages to other vehicles (e.g., in Fig. 8). However, due to the unpredictable network topology, interference, packet collisions, and hidden nodes, multihop transmissions over V2V networks can be very challenging.

A cluster-based communication scheme in V2V environment was presented in [60]. If a vehicle can receive a valid invite-to-joint (ITJ) message from a cluster head within a specific time period, it will become a cluster member; otherwise, it will become a cluster head by itself. A cluster can be merged with another cluster if the cluster head receives a valid ITJ message from a neighboring cluster head which has more members. For intra-cluster communication, cluster members can send data to the cluster head by using a centralized management scheme, and for inter-cluster communication, data gathered by the cluster head are sent to another head using contention-based MAC protocol. Furthermore, this proposed scheme uses two transceivers and different channels in order to make a vehicle be able to simultaneously transmit request/control messages, real-time data, and non-real-time data resulting in reduction of time delay for safety messages.

5.2. MAC protocols

For V2R communications, MAC protocols define how the vehicular nodes and the RSUs share common radio channels and for V2V communications, MAC protocols define how the vehicular nodes share channels to transmit data among them. Hidden terminal problem caused by infrastructures along roadside, frequent handoffs caused by high mobility of vehicles and high dynamic of topology, fairness in channel access are challenging issues for efficient MAC design [7,61,62]. The traditional MAC protocols (e.g., ALOHA,

CSMA, CSMA/CA, and IEEE 802.11 MAC) may not be suitable for vehicular networks with high node mobility [61]. The new IEEE 802.11p (or WAVE) standard enhances the IEEE 802.11 MAC in order to support rapid movement of vehicles [6].

The MAC protocols for vehicular networks can be classified into the following categories:

- *Centralized or distributed MAC protocols*: With a centralized MAC protocol, the decision of when and how the channels are accessed is determined by a central controller (e.g., scheduling in [58,60]). With complete node information, a centralized MAC protocol can be optimally designed at the expense of overhead needed to acquire such information. A distributed MAC protocol, on the other hand, determines how the channels are accessed based on local information (e.g., contention in [60,61]). Despite decreasing overhead, a distributed MAC protocol is usually not optimal due to incomplete node information. While centralized MAC protocols would be preferable for V2R communications, distributed MAC protocols would be more suitable for V2V communications.
- *Single or multiple channels*: In presence of multiple channels (possibly different technologies), a MAC protocol needs to select channels to satisfy the application requirements. For example, a high data rate and possibly a high attenuation-sensitive channel (e.g., in 5.8 GHz) should be used for typical data exchange, while a low data rate (usually more robust) channel (e.g., VHF or UHF) should be used for transmitting control and safety messages [57].
- *Single or multiple RSUs*: When considering multiple RSUs, the MAC protocol needs to control the handover process when a vehicle moves from one roadside base station to another. For example, a distributed MAC protocol was designed in [61], which quickly associates and disassociates a vehicular node with an RSU.

5.2.1. MAC Protocols for V2R Networks

The IEEE 802.11-based MAC protocols will not be suitable for V2R communications due to long communication range, low efficiency in multihop transmission, and high degree of movement of vehicles on the road [63]. A new MAC protocol for V2R communications was proposed in [61] which combines the concepts of both centralized and decentralized channel access. It provides prioritized access to nodes to quickly reassociate or disassociate with the access points. Also, it aims at minimizing packet delay while ensuring fairness among the nodes.

In a V2R communication scenario, a vehicular node needs to be served by an RSU within a limited period of time. However, the RSU may not be able to serve requests from all vehicles within a limited time because of high mobility of vehicles, large amount of requests from vehicles, or limited broadcast range. Therefore, a scheduling algorithm would be required at the RSU to make decision on the sequence in which the vehicles will be served. Most of scheduling algorithms proposed in the literature are based on parameters such as data size, deadline, request arrival time and frequency etc.

In [58], a scheduling algorithm called Maximum Freedom Last (MFL) scheduling algorithm was presented. The design goal of MFL algorithm is to minimize the system handoff rate, while the effective system utilization is maximized. The scheduling algorithm uses cell dwell time and remaining transmission time as parameters to make a priority queue. A larger remaining cell dwell time implies a lower service priority. A larger transmission time implies a higher service priority. The MFL scheme minimizes the handover rate subject to a given delay constraint. Also, the MFL scheduling scheme was shown to perform better when compared with the first-come-first-serve (FCFS) and earliest-deadline-first (EDF) scheduling algorithms.

A scheduling algorithm named $D * S$ was proposed in [64] for V2R communications in order to provide efficient data access by considering service deadline and data size. There are two main concepts in this algorithm. First, given two requests with the same deadline, the vehicle which requests for a smaller amount of data should be served first. Secondly, given two requests asking for data with same size, the vehicle with an earlier deadline should be served first. The algorithm was shown to outperform other scheduling algorithms such as first-come-first-serve, first-deadline-first, and smallest data size first algorithms.

In an IEEE 802.16/WiMAX-enabled V2R communications scenario, the centralized WiMAX MAC can be used to provide broadband access to vehicles on a motorway scenario [65] while ensuring fairness guarantee in bandwidth usage. Also, the WiMAX MAC can be configured to operate in point-to-multipoint (PMP) or mesh mode depending on the application and availability of infrastructure. In order to increase effective coverage of the wireless access network, a new system architecture called Wi-FAN (WiMAX fast-moving access network) was presented in [65].

5.2.2. MAC protocols for V2V networks

For V2V communications, the latency of medium access should be low enough to achieve the desired application requirement (e.g., a maximum delay of 100 ms for safety applications as defined by the Vehicle Safety Communications Consortium). As has already been mentioned, a distributed MAC scheme is more suitable for V2V communications. IEEE 802.11p standard-based MAC, which allows a transmission range up to 1000 m, is a candidate MAC scheme for distributed V2V communications [2,8,60,66]. With IEEE 802.11 MAC, adaptation of the contention window (CW) size and the physical layer data rate can enhance broadcasting performance in V2V communications [67]. By considering the estimated number of vehicles in the surroundings, the adaptation of CW size helps decreasing the probability of collision and decreasing the transmission delay. Moreover, the data rate selection improves network capacity and helps in situations of channel congestion. The combination of both adaptations of CW size and the data rate outperforms the performance achieved by the traditional IEEE 802.11 system.

For a clustered multihop V2V network (Fig. 9), a centralized multi-channel MAC protocol was proposed in [60] for intra-cluster communication. A cluster head uses centralized time-slot based

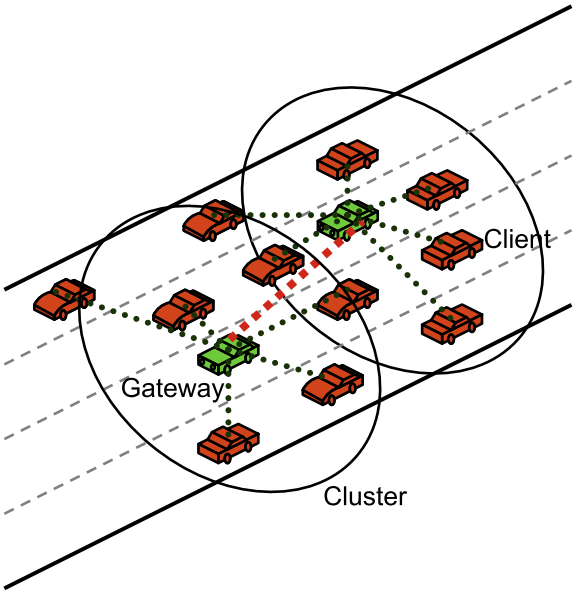


Fig. 9. A model of cluster-based transmission in V2V networks.

scheme assignment for the cluster members to transmit real-time data over a channel and non-real-time requests over another channel. However, each cluster head uses the contention-based IEEE 802.11 MAC protocol to deliver real-time and non-real-time data over two different channels.

Based on a survey of the existing MAC protocols, the authors in [4] concluded that more efforts are required to put them into practice. Besides IEEE 802.11, MAC protocol based on UTRA TDD in the unlicensed 2010–2020 MHz band [21], could be a promising solution for V2V networks.

5.3. Data dissemination protocols

In order to make vehicles run safety applications, many different data dissemination mechanisms were proposed in the literature. The main purpose of these mechanisms is to deliver the safety data to the intended recipients of the data in a low-delay reliable manner. Due to unpredictable network topology, interference, packet collisions, and hidden nodes, data dissemination over vehicular networks can be very challenging.

In [2], a safety data dissemination mechanism for intra-platoon cooperative collision avoidance was proposed. A platoon is a group of vehicles that are connected to each other directly or by multihop transmissions. In order to reduce the amount of broadcast traffic and to enhance the delivery rate, an implicit acknowledgment mechanism is used. Unlike other studies, in this paper the impact of the proposed mechanism was evaluated on vehicular crash performance, rather than on conventional networking performance. An issue with this mechanism is that since both safety applications and traffic applications are using the same frequency channel in a distributed manner, the latency of the packets depends on the overall traffic and safety applications traffic. Any variation in the overall traffic may cause the delay to go beyond the tolerable threshold.

The data dissemination mechanism proposed in [24], called urban multihop broadcast (UMB), removes the need for beaconing and it also addresses the problem of data dissemination in the intersections. Unlike flooding-based protocols [2], in UMB each vehicle forwards the packet only to the node in the furthest segment of its radio transmission range. At the intersections, the packets are broadcast with the help of repeaters. UMB aims at addressing the broadcast storm, hidden node, and reliability problems. In order to get rid of repeaters and make the mechanism infrastructure-independent, the authors of UMB proposed an ad-hoc extension of UMB mechanism called ad-hoc multihop broadcast (AMB) [26], in which within the intersections, the vehicle closest to the intersection is responsible for forwarding the broadcast packet to the other road segments instead of repeaters. However, AMB fails when the message in an intersection leaves the intersection without being disseminated along all the intersecting road segments. Therefore, an enhanced intersection mode data dissemination mechanism (EIDD) was proposed in [27] that keeps emergency messages in the intersection long enough to ensure that the messages are forwarded to all the intersecting road segments.

In the data dissemination mechanism studied in [25], vehicles use periodic beacon messages to report their location, direction and velocity to each other. In this mechanism, called data pouring (DP), the broadcast packet is consecutively broadcast along the road by each forwarding vehicle to the furthest vehicle in its neighbour list in the data dissemination direction. This periodic data pouring, however, results in high data traffic in the network. To reduce the data traffic and improve the data delivery ratio, another mechanism called data pouring with intersection buffering (DP-IB) was proposed where instead of periodically pouring the data on the roads, data is only buffered at the intersections and is periodically rebroadcast to the intersecting secondary road segments by means of simple devices called relay and broadcast station.

In [68], a data dissemination mechanism was proposed which can cope with extreme traffic situations, such as high traffic or low traffic. Due to the bi-directional lane mobility model employed, the vehicles in different directions can be considered to be in different clusters. In this mechanism, if the relaying vehicle is moving in the same direction as the source and has one neighbour behind moving in the same direction, it forwards the packet to that vehicle. Otherwise, it forwards the packet to one vehicle in the opposite direction. If the relaying vehicle is not connected to any of the vehicles (in the same or opposite direction), it holds the packet until it receives a hello packet from any vehicle or until the packet expires. To handle the broadcast storm problem [70] in forwarding the packet, the broadcast suppression scheme in [69] was employed.

5.4. Data aggregation protocols

SOTIS [28] and TrafficView [29] (introduced in Section 1) aim at providing vehicles with traffic information within the 50–100 km radius. However, due to limited system capacity, each vehicle is only allowed to disseminate a small packet in every beaconing period. To include as much traffic information as possible in the traffic packets that the vehicles broadcast, every traffic information system (TIS) employs a data aggregation algorithm. In TrafficView, the aggregation algorithm considers the vehicles in close relative distances to minimize the error resulting from aggregation, and the timestamp of an aggregate is the minimum generation time of the considered records. In order to improve efficiency and reliability, [71] proposed a hierarchical data aggregation algorithm, called quad-tree aggregation algorithm, which allows the generation of traffic information aggregates for areas of variable geographic extensions.

In the quad-tree aggregation algorithm, the map is divided into non-overlapping areas by an overlay grid of a hierarchical quad-tree architecture instead of road segments. The raw atomic information units, which are the number of free parking spots counted and periodically broadcast by the RSUs, constitute the aggregates of the lowest hierarchical level, and four aggregates of a lower level are integrated into a higher level aggregate, and the timestamps of the aggregates are the average generation times of the atomic units. To deal with the limited system capacity, only a fixed number of aggregates of each hierarchical level are broadcast by any vehicle. The aggregates are prioritized based on their relevance which is computed by taking their age and distance into consideration. In SOTIS, TrafficView, and quad-tree aggregation algorithm, when several aggregates with different but overlapping knowledge for the same segment or the same area are received, the one with the newest timestamp is taken into account and the rest are dropped. However, the timestamps are the generation times of the aggregates or the minimum or average generation times of the atomic units, and this makes a direct comparison of the aggregates rather inaccurate and unreliable because the contained data may be incomplete or not up-to-date. To overcome this problem, [72] proposed another hierarchical data aggregation algorithm in which multiple aggregates for the same area can be merged and none of them is dropped. Instead of having all the data for generating the aggregates first, the data is incorporated into aggregates on-the-fly while they are being passed around. In this algorithm, the distinct traffic values, e.g., the velocity or position of the vehicles or the number of parking spots, are mapped into probabilistic data structures called Flajolet–Martin sketches [33]. The sketches are merged by a simple bitwise OR guaranteeing that adding already present elements again does not change the results. In order to remove old observations, a time-to-live counter is assigned to

each bit of the sketches that counts down one unit before each broadcast, if not yet zero, or it can be refreshed by a newer observation.

5.5. Routing protocols

The employment of a routing protocol is inevitable in many vehicular applications. These include, for example, a scenario in which a vehicle inquires information about traffic condition or available facilities on a road segment or a scenario where a piece of information on the Internet is required, or applications in which two vehicles need to have a peer-to-peer communication. Broadcast routing, which disseminates information to a set of vehicular nodes far from each other, will be a supporting mechanism for many ITS applications. Many routing protocols for the vehicular ad-hoc networks were proposed in the literature [73]. In [73], the authors observed that only a few of the existing routing protocols for inter-vehicle networks are able to handle the requirements of safety applications. This is primarily due to the large overhead incurred for route discovery and route maintenance for highly mobile uncoordinated vehicles. An important group of routing protocols for ad-hoc networks is topology-based routing protocols which needs an establishment of an end-to-end path between source and destination before sending any data packet. Due to fast changes in the network topology and highly varying communication channel conditions, the end-to-end paths determined by regular ad-hoc topology-based routing protocols are easily broken. Therefore, modifications of regular topology-based routing protocols were proposed to make them applicable to VANETs [74,75], and completely new topology-based routing protocols were proposed as well [76–78].

In [76] a topology-based routing protocol called MURU was proposed which assumes that an end-to-end path can be obtained by selecting the most robust paths with lowest breakage probabilities using mobility information. Regarding the number of nodes which might lead to network partitioning, and highly varying communication channel through the coverage area of the network, this assumption, i.e., the existence of an end-to-end path, may not always be valid.

In [78], a path selection scheme called receive on most stable group-path (ROMSGP) was proposed. Vehicles are grouped together according to their velocity vectors which include positions, directions, speeds and digital mapping of the roads and the vehicles belonging to the same group are given priority in forming the end-to-end routes to ensure the establishment of more stable routes. In other words, the selection of the stable path is based on the set of available paths which have the highest link expiration time (LET) value. Simulation results showed that ROMSGP can reduce the number of path breakage and control overhead.

Another group of routing protocols for ad-hoc networks is position-based or geographic routing protocols which are known to be more scalable since the forwarding decisions are based on the current neighbors of the forwarding node and the next forwarding nodes are not initially determined. However, these protocols fail in a considerable number of scenarios because they do not consider information on the roadmaps or vehicles' mobility patterns in their decision-making procedure. To overcome this problem, spatially aware routing (SAR) was proposed in [79] where the routes are computed by Dijkstra's algorithm on the basis of roadmap information. The protocol fails when the packets are forwarded over a disconnected route including links with no vehicles, i.e., with no connectivity. Anchor-based street and traffic aware routing (A-STAR) was then proposed in [80] which employs the information on city bus routes to identify an anchor path with high connectivity for packet delivery and takes advantage of a new recovery strategy for packets routed to improve the performance of the protocol. Although in this protocol the chance that more connected routes are selected increases, there is still the possibility that the packets are forwarded over disconnected routes for some periods. Furthermore, pushing all the data traffic towards main roads increases the chance of data traffic congestions over those roads. To overcome this problem, the authors in [81] proposed a vehicle-assisted data delivery protocol. In [81], both the traffic pattern and road layout are used by a forwarding vehicle to find the next road to forward the packet with the purpose of minimizing the end-to-end data delivery delay by using a carry-and-forward strategy.

Although many studies showed that in vehicular communications position-based routing protocols outperform topology-based routing protocols, in [82], a position-based routing protocol called connectivity-aware routing (CAR) was proposed which uses an end-to-end route discovery process, i.e., a topology-based approach to locate the destination. However, the discovered route contains a set of anchor points formed by the velocity vectors of the relaying vehicles along the path. In other words, CAR is indeed an integration of position-based and topology-based routing protocols which combines finding the location of the destination as well as determining the connected path between the source and the destination. It also includes a path maintenance mechanism called guard to keep track of the current position of the destination.

In [83], empirical vehicle traffic data (measured on I-80 freeway in California) was used to develop a comprehensive analytical framework to study the disconnected network phenomenon and its network characteristics. It was shown that depending on the

for more bandwidth then the available capacity. One way to address this problem is to increase the bandwidth but this is usually not cost-effective because quite often congestion arises due to the inappropriate allocation/utilization of resources. Another approach is to fairly share the available bandwidth among the users without causing congestion, i.e., congestion avoidance with efficient bandwidth management. For example, MAC queues were manipulated to deal with channel congestion in a contention-based channel access scheme [90]. This MAC protocol has application to the performance of Emergency Electronic Brake Light with Forwarding (EEBL-F) application in congested scenarios [90] which addresses the safety and traffic information issues mentioned in Section 2.

Streaming traffic (e.g., streaming video) is another important application in the future AHVN architecture that would require a steady supply of bandwidth to provide un-interrupted service. Since many of the applications in wired networks are already TCP (Transmission Control Protocol)-based, it is natural to extend TCP to wireless networks. However, it has been observed that TCP performs less efficiently in wireless networks compared to wired networks (e.g., [86]). In a wired network, TCP interprets data loss as the main reason for congestion [88]. This assumption holds well in reliable wired networks. In wireless networks packet losses may occur due to link failure, high bit error rate, handover or any other reasons [87]. When a packet loss occurs due to such an event, triggering the congestion control algorithm may result in un-necessary reduction in the source sending rate. Therefore, considering packet drops as the major cause for congestion is not efficient in wireless networks especially for streaming multimedia transmission [93].

In order to address the problem of data traffic congestion in VANET, we need an algorithm that can regulate all types of modern Internet traffic (like streaming multimedia) while considering various congestion factors in wireless networks. Below is the classification of two types of existing congestion control algorithms. Discussion of some potential candidates is also provided.

5.6.1. Window-based congestion control algorithms

The dominant window-based congestion control algorithm is TCP, which plays an important role in order to address the problem of congestion [91]. As mentioned earlier, TCP interprets packet loss as an indication of congestion. It relies on the AIMD (Additive Increase Multiplicative Decrease) [88,92] technique to address the congestion problem. However, such a practice is not efficient for streaming multimedia transmission [93].

In order to improve the performance of TCP, new features were added to the exiting protocol. The well-known TCP variants are Tahoe, Reno, and NewReno. TCP Tahoe [88,94] includes slow start and congestion avoidance techniques. TCP Reno [95] was developed by adding two additional features to TCP Tahoe – fast retransmit and fast recovery. This technique detects packet loss and performs error recovery before the transmission timer expires. TCP New Reno [96–98] is an improved version of TCP Reno. TCP New Reno provides better thresholds for fast recovery and improves retransmissions. TCP New Reno is the most commonly implemented algorithm. For all the TCP variants discussed so far, the TCP window size exhibits a saw-tooth behavior resulting in source sending rate fluctuations. Furthermore, TCP along with its variants assumes packet loss as the main reason for congestion which is not appropriate for wireless networks.

TCP and its variants discussed above are source-based techniques. AQM (Active Queue Management) is a router-based congestion avoidance mechanism to improve the performance of TCP congestion control. A well-known example of AQM is RED (Random Early Detection) [99]. Traditional tail-drop techniques buffer packets until the buffer is full. Once full, the node drops any new packets leading to congestion. As a result, there is an unfair distribution of buffer among traffic flows. Buffering may also lead to an increase in RTT (Round-Trip Time), thus degrading the quality of service. RED addresses these problems by dropping packets with a probability and maintaining the average queue size between the configured minimum and maximum thresholds. When the queue is empty, all incoming packets that cannot be serviced immediately will be queued. As the queue grows, RED will start dropping packets with a probability that increases with the queue length. It has been observed that the throughput of RED is sensitive to traffic load and decreases when the queue size is greater than the configured maximum threshold [100,101]. Furthermore, RED does not perform well in wireless ad-hoc networks. NRED was proposed to deal with the problems of RED in wireless ad-hoc networks [102]. BLUE [103] and FRED [104] schemes improve RED by adjusting the packet drop probability. AVQ (Adaptive Virtual Queue) [106] makes use of a token bucket algorithm to provide AQM. Most of these protocols are based on heuristics without strong theoretical backing.

Like the TCP variants above, the general observation is that window-based protocols (e,g, RED, BLUE) exhibit a saw-tooth behavior which leads to sending rate fluctuations, and are not suitable for streaming multimedia transmission.

5.6.2. Rate-based congestion control algorithms

Rate-based congestion controllers adjust the source transmission rate by controlling the size of the TCP window at the source. Source transmission rate is directly proportional to the TCP window and inversely proportional to the RTT. As a result, the size of TCP window can be derived from the source transmission rate. Rate-based controllers are well-suited for streaming multimedia applications [93]. TFRC (TCP Friendly Rate Control) [108] is a rate-based controller at the source for unicast traffic. As in the traditional AIMD, TFRC does not halve the sending rate in response to congestion notification. This makes TFRC a candidate protocol for streaming multimedia transmission in wired network. TFRC resides at the source and provides an equation-based congestion control mechanism for unicast traffic. The proposed equation is a function of packet loss observed during the transmission. Unfortunately, considering only packet loss is not reasonable for wireless networks.

Rate-based controllers can also use AQM at the intermediate nodes to participate in congestion management [109]. The algorithm residing at the intermediate node calculates the source sending rate based on congestion and converts it to TCP window to manage traffic. The TCP rate control improves the TCP performance by controlling the source sending rate. The sending rate of the TCP source is derived from window size, round-trip time, and the rate of acknowledgements. TCP rate control maintains states per TCP flow and provides protection against misbehaving TCP sources. The window size can be calculated as a function of input-output rate mismatch in order to match the servicing capability or bandwidth of a node. In another approach, the network layer conveys available bandwidth and propagation delay measurements to TCP sources, which computes the source window using bandwidth delay product. The EXACT (Explicit rate based flow control) [110] presents an end-to-end flow control scheme where the intermediate node conveys the source rate to the end host in the control header of each packet. It relies on MAC and transport layers to address the problem of congestion. The source sending rate is calculated based on current measured bandwidth of the outgoing links and the current rate of information flow going through the router.

The Adaptive Proportional Integral (PI) Rate Controller [111] is a rate-based controller that supports best-effort traffic in the Internet. It employs control theory and AQM in order to deal with congestion. The controller calculates the source sending rate based on instantaneous queue length of the intermediate router and adver-

tises it to the sources using the acknowledgement message. The adaptive feature of the controller allows it to self-tune only when there is a dramatic change in the network traffic. The adaptive PI rate controller does not interpret packet loss as the reason for congestion. The controller is capable of providing a steady throughput at the source which is well suitable for multimedia streaming.

The utility-based control can be a variation of rate-based control method. The source node adjusts its transmission rate based on feedback network congestion information and utility function. The UBPFCC (Utility-Based Packet Forwarding and Congestion Control) algorithm [112] assumes broadcast to be the dominant form of communication in VANET and addresses congestion caused by broadcast applications. This approach is not appropriate for transaction-based applications that can also exist in VANETs, and either broadcast or transaction-based applications can be the reason for congestion. The algorithm utilizes a utility function and encodes the utility information in each data packet. The average utility value is then calculated for each individual node and based on this the available data rate is shared.

5.7. Cross-layer protocol design in vehicular networks

Traditional layered approach relies on adapting the communication layers independently from other layers. The arguments that support layered approaches consider that designing independent protocols for each communication layer will create long-term solutions. However, this type of implementation has been long criticized as being rigid and incapable of having proactive change to short term changes in network environment, and the excessive overhead from layer to layer represent degradation in throughput.

As a different approach, cross-layer design makes use of feedback information from lower layers to help the transport layer perform better under network congestion [113]. This is dealt with the detection, control and corresponding reaction to particular network conditions such as channel errors, link contention and route failures. By exploiting this information, the network itself will be able to determine the current load situation and protect itself from congestion [113]. There can be different combination of layers involved in this approach such as application and network layers, and transport and link layers. In fact, the TCP suit has not been strictly a layered protocol to start with. Non-linear design can be used to study the tradeoff of the power control in the physical layer and the transport layer congestion in a multihop network such as a VANET [114].

In the area of MAC protocols for VANETs, some starting points for proposals dealing with novel concepts like cross-layer exploitation of IEEE 802.11-based MAC mechanisms and dynamic clustering for efficiency and realiability of V2V multihop broadcast, multichannel MACs, and practical performance issues in different scenarios can be found in [115–117]. In particular, [115] illustrated the design and analysis of a fast multi-hop forwarding MAC and clustering scheme for VANETs which is compliant with IEEE 802.11 DCF systems. A multichannel MAC protocol was proposed in [116] for high density VANETs using directional antennas. The proposed scheme was observed to provide a high spatial reuse and high probability of reliable transmission. A simulation-based cross-layer (MAC and routing) performance study was presented in [117] for IEEE 802.11 MAC (i.e., CSMA/CA), and ADHOC-MAC which is based on reliable reservation (RR)-ALOHA used in CalTALK and FleetNet projects [21,22]. Efficient design of cross-layer protocols for VANETs remains as an open problem.

5.8. Security protocols

Security is among the most important aspects of vehicular networks. All messages exchanged between OBUs and RSUs must have the standard properties of authentication and non-repudiation, i.e., that the source of each message can be authenticated, and also that the originator of the message can't subsequently deny sending the message. Contents of the message must be checked for integrity if necessary. All safety-related messages must be delivered with bounded delay. Senders of safety messages must have the right to preserve their privacy so that their identity can be revealed if necessary only to legal authorities. In this context, wireless location privacy protection [118] and secure location verification [119] are two important issues in vehicular ad hoc networks. Furthermore, some of the messages that are encrypted may need to be examined later for forensic evidence. On the other hand, all participants in a vehicular network may have incentives for misbehavior, which may easily result in some kind of security attacks.

There has been a significant research activity in listing and analyzing potential security attacks in vehicular networks [120–123,4,124–129]. Several possible security threats in VANETs were identified in [124]. For example,

- Drivers might attempt to modify speed and position information to avoid liability for the accidents.
- Drivers could also modify congestion information in order to get faster to the destinations.
- Bogus RSUs may be placed along the road to transmit false information about traffic congestion, thus causing the drivers to make wrong decisions, or perhaps to prevent transmission of safety messages which amounts to a Denial of Service (DoS) attack.
- An attacker may cause channel jamming or inject dummy messages to bring down the network (DoS attack).
- An attacker may pretend to be another vehicle by using false identities (*Masquerading*).
- Industrial vendors and service providers that manufacture and/or operate RSUs and servers may collect and sell information about the vehicles' driving patterns, traffic parameters, and accidents.
- Police officers might abuse their authority using their networking privileges.

All these security attacks indicate that attacks should come mostly from 'insiders,' and that no participant – be it an OBU, RSU, or even a network server – should be fully trusted. There is also a possibility of attacks by outsiders who can attempt to disturb traffic safety by replaying old messages, or even launch a DoS attack by flooding the area with bogus messages. The obvious conclusion is that appropriate security mechanisms must be deployed in order to raise security assurance of a VANET. Of course, the security mechanisms must comply with the AHVN communication architecture described before.

In [124], it was concluded that, given the nature of the VANETs, the existing security solutions cannot be readily applied to these networks. The requirements for a security system for safety messaging in a VANET are as follows [124]: authentication, verification of data consistency, availability of a robust communication channel, tamper evidence mechanisms at the vehicular nodes and RSUs, non-repudiation, privacy, and real-time constraints. To address these security requirements, a number of proposals for a security architecture have been published in recent years. Most of the proposals use some form of public key infrastructure (PKI), possibly modified to cater to the characteristics of a vehicular network, where the certification authority (CA) is placed on information servers, while RSUs and OBUs obtain certificates with public/private key pairs. However, some approaches use a hybrid of PKI and symmetric key architecture, based on pre-established secret keys between components of infrastructure. Symmetric keys thus shared are subsequently used to generate message authentication

code (MAC), using keyed hash function HMAC (Hash Mutual Authentication Code) technique. The main motivation for the development of the hybrid security architecture is to decrease the computational overhead of generating and verifying digital signatures in PKI architectures.

It was pointed out in [125] that the overall security in a vehicular network can be enhanced by doing local plausibility checks in vehicles (e.g., internal sensors) and the RSUs. These checks can include, for example, comparison of received information to sensor data and evaluation of messages from different sources about a single event.

We list the main categories of security architectures below, the main difference among them being the level of trust built into OBUs, RSUs, and application servers, as well as the level of ID and location privacy offered to the drivers. Note that privacy is conditional, since in the case of dispute legal authorities have the right to reveal the IDs of OBUs and RSUs involved in accident. All approaches assume that vehicle has tamper proof hardware (TPH) to store certificates or/and elements of shared secret.

5.8.1. PKI-based architectures

One of the pioneering proposals in this area is [130] where Drive Ad Hoc Networking Infrastructure (DAHNI) was proposed including PKI infrastructure for managing public/private key pairs. Authentication and integrity is achieved using RSA encryption for digital signatures.

In [131], the authors presented a PKI infrastructure within the SecCar project. It is based on a cluster communication model, where cluster heads sign the messages and transmit them to individual recipients.

The next step was done in [120], where a vehicular public key infrastructure was proposed, including a Certificationing Authority (CA) which issues public/private key pairs to vehicles. Authors assume that vehicles contain electronic identity in the form of electronic licence plate (ELP) issued by the government and/or electronic chassis number (ECN) issued by the vehicle vendor. To preserve privacy and prevent location tracking, each vehicle is given a large set of short-lived anonymous key certificates which do not contain the vehicle ID. To prevent location tracking, public/private key pairs have to be periodically changed. The authors evaluated the computational complexity and size of signatures for three Public Key Cryptosystems (PKCS). Proposed digital signature is based on ECDSA (Elliptic Curve Digital Signature Algorithm), which helps to reduce the packet size.

A slightly more secure architecture was proposed in [132] where vehicle certificates are blindly signed by the CA, so that insiders cannot easily establish the link between the vehicle ID and issued certificate(s). This link is escrowed [133] by multiple authorities.

In [123,134], the PKI infrastructure is enhanced with two cryptographic techniques that improve drivers' privacy. Namely, for the communication scenario in which a group of OBUs communicates with the RSU, group signature is used to secure the communications among OBUs in the communication group. Messages are securely and anonymously signed by the OBUs so that neither RSU nor any other eavesdropper is able to resolve the actual identity of the signer. Identities of the signers can be recovered by the authorities though. Messages sent by the RSU to the OBUs are authenticated by digital signature, using ID-based cryptography.

Work reported in [135] is an extension of [120] in the sense that anonymous public key certificates are associated with OBU's pseudonyms which are not issued by the same authority (CA) as proposed in [136]. As a result, linking messages under different pseudonyms becomes increasingly hard over time and space. This work also defines the rules for changing the pseudonym, i.e., the public key. These rules require changing MAC address and IP address of the OBU in order to prevent tracking.

5.8.2. Hybrid security architectures for vehicular networks

The security architecture proposed in [137] is based on shared, long-lived vehicle pseudonyms. They are pre-installed on RSUs and OBUs. The link between the vehicle pseudonym and its real identity is kept in trusted servers. Long-lived pseudonyms are used to derive session keys which are used to provide packet authentication code using HMAC technique [133].

A modification of hybrid PKI security architecture was discussed in [138]. In this proposal, a trusted third party (TTP) which plays the role of the CA, allocates a number of pseudonym certificates to each vehicle. Pseudonym certificates are preloaded in the TPH, together with the root certificate of the CA. After the certificate exchange, the two neighbors can securely exchange a secret symmetric key.

In [139], a security architecture for application services in a vehicular network was proposed based on Kerberos. The architecture supports authentication, authorization, and accounting. The user submits a request for service to the Kerberos Server at the service provider (SP) site. If the request is successful, the SP issues a Ticket Granting Ticket (TGT) which contains authorization for information services. The user then submits the TGT to the Kerberos proxy residing at the RSU in order to receive an IP address from DHCP server and public key certificate. The public key is used afterwards for the generation of symmetric keys between OBUs, for the purpose of mutual authentication.

A hybrid architecture in which the OBU does not trust public servers was proposed in [140]. This architecture is characterized with group-based anonymous authentication protocol in which an OBU obtains the RSU's certificate, and then uses the RSU's public key to encrypt and submit group session key and other authentication parameters to the RSU. An extension of this approach was proposed in [141], where each vehicle is assigned a symmetric key pool.

The framework from [120] was combined with the TESLA broadcast authentication protocol [142] to develop the TESLA based Secure Vehicular Communication protocol (TSVC) [143]. In this architecture, an OBU is allocated a large number of short-lived anonymous certificates, like in [120], but during the lifetime of each certificate messages are authenticated using a hash chain [144]. The hash chain for each certificate is initiated using a random seed S. Each hash value is used as a secret key to generate the HMAC for a number of packets, and released with a delay of δ so that HMAC can be verified. Therefore, a digital signature with anonymous keys is needed only for the first packet in the chain sequence, and the computational burden of verifying packet integrity is decreased.

5.8.3. Enhancing security by data aggregation, validation, and correction

The overhead incurred in implementing a security mechanism can be reduced (and hence the channel efficiency can be improved) through data/message aggregation in a group communication environment [126]. Data aggregation can also contribute to better data correctness and hence to a higher level of security. In [126], the authors proposed three aggregation techniques for the relaying vehicles (i.e., group leaders). These are based on *combining signatures* from a group of vehicles reporting the same event, using *overlapping groups* with each geographically-predefined group having its own symmetric key, and *dynamic group key creation*. With secure aggregation mechanisms, the effects of vehicle density and speed on the bandwidth consumption and delay were observed by simulations.

The problem of validating aggregated data in V2V networks was addressed in [127]. The authors proposed a solution to this problem based on PKI-based authentication the main idea of which is to use random checks to catch the attacker probabilistically, and discouraging the attackers by imposing a high penalty. After an aggregated message has been sent, to validate the message, the aggregator is asked to provide a randomly-chosen original signed message. The overhead of the proposed approach is small in terms of communication costs.

A general sensor-driven approach to detect and correct maliciously introduced errors in VANET data was proposed in [129]. In this approach, each node maintains a *model of the VANET* containing its knowledge on the network, and it tests the validity of data received from other nodes against this model. The sensor data collected by the nodes are shared with immediate neighbors and propagated to a neighboring region.

A distributed method to detect forged position information in VANETs was proposed in [128]. The main idea is to calculate a trust value for the other nodes based on the observations over time on the different network parameters such as maximum transmission range, maximum speed, maximum node density. Although the proposed method does not entirely prevent the malicious nodes to forge the position information, it however significantly reduces the possibilities for attackers using falsified position information.

The problem of design, analysis, and implementation of efficient data aggregation, validation and correction in VANETs still remains as an open problem.

5.9. Privacy protocols

As has been mentioned before, drivers have the incentive to 'try to bend the rules' and avoid liability for violating traffic rules, by modifying the information about their speed, position, acceleration/deceleration, and other relevant variables in the safety messages, in order to avoid liability. On the other hand, as noted in [121], the majority of drivers is honest and would not feel comfortable tinkering with their OBUs. Such drivers will gladly contribute safety messages but under the condition that these messages will not reveal their ID, name, location and driving patterns to unauthorized third party. However, drivers' privacy in a VANET is conditional, since in case of a dispute it can be revealed by legal authorities. This issue has launched significant research activity and basically all aforementioned VANET security architectures differ in their view and implementation of driver's privacy.

Driver's privacy is generally achieved using pseudonyms [136], which can be time- or geographically based.

Time-based pseudonyms were defined in [145] as:

$$P_X(t) = \mathrm{HMAC}_{K_X^-}(\mathrm{ID}_X, t)$$

where ID_X is the real identity of the OBU (and, by extension, the vehicle) X, $P_X(t)$ is the vehicle pseudonym calculated at time t, HMAC is the keyed hash function, and K_X^- is the secret key. Similar approach was used in [146] where pseudonyms change over time. Mapping between pseudonyms and real identities is performed by the trusted authority which stores the real identities and can, thus, easily perform the translation in either direction.

Geographically based pseudonyms were proposed in [120,132,135,143]. These pseudonyms can be implemented as a large set (probably 43800 certificates per OBU) of anonymous certificates with public keys, which the OBU changes after some traversed distance. Legal authorities maintain the link between the set of anonymous certificates and the ID of the OBU which is equal to electronic licence plate. An interesting technique, called Caravan, for changing geo-based pseudonyms was proposed in [147]. This approach is based on a navigation group of vehicles sharing the same geographical zone. All vehicles within the group deploy a random silent interval before changing the pseudonyms. After the silent period, the vehicle designated as Group Leader transmits the updates of pseudonyms to the members of the navigation group. In this manner, mapping of new pseudonyms to vehicle IDs by an unauthorized third party is prevented.

Similar approach to anonymity was proposed in [121], where anonymizer servers are placed at RSUs. When vehicle V wants to change its pseudonym and its public/private key pair $K_V,\ K_V^{-1}$, it will interact with the RSU/anonymizer R in the following way:

$$R \rightarrow V : N$$
$$V \rightarrow R : K_V, \{N\}_{K_V^{-1}}$$
$$R \rightarrow V : \{K'_V, K_V'^{-1}, T, \{K'_V, T\}_{K_R^{-1}}\}_{K_V}$$

where N is a random nonce, T is the timestamp, and pair $K'_V,\ K_V'^{-1}$ is the new set of keys. The problem with this approach is that the RSU has to be properly authenticated by the vehicle. Moreover, there is the problem of tracking the identity of a vehicle through the set of RSUs, if it has liability issues. Therefore, it would be appropriate if the vehicle submits its real identity to the anonymization server, as indicated by the authors in [121].

The work in [135] has the potential to achieve a high degree of untraceability. However, it assumes existence of a pseudonymity resolution authority (PRA), the implementation of which is currently vague. If the role of the PRA is played by the CA, this framework is virtually identical to the one described in [120]; furthermore, about the same level of location privacy can be achieved using the proposal in [143]. However, the price of privacy for these techniques is that since the number of certificates per OBU is large, detecting an OBU which has sent false message requires searching the table of certificates which has an enormous number of entries (43,800 times the number of cars in the province/country).

Yet another privacy preserving technique was presented in [138] where each new member in the vehicle group submits its own certificate together with x other (dummy) certificates. In this manner, the attacker will not be able to trace the vehicle identity. However, all existing neighbors would have to encrypt all their messages with all public keys (or all symmetric keys in hybrid variant), which makes this approach costly and not scalable.

Finally, the GSIS scheme [134], which offers a high degree of privacy using group signature technique, has high computational and communication cost.

6. Open issues and research directions

The objective of the AHVN architecture is to integrate the diverse wireless access technology so as to provide an "always best connected (ABC)" communication capability that is secure, reliable and cost-effective. Such a communication platform is not currently available but is highly desirable to advance the capabilities of future ITS applications. Efficient protocol solutions (e.g., for medium access control, radio resource management, radio link control, Internetworking between DSRC, 3G cellular, and WiMAX networks, and end-to-end transmission control) will be essential for cost-effective deployment of AHVN. The protocol solutions should consider the dynamics of a highly mobile and potentially sparsely connected network of vehicles. Addressing (and hence routing) is a difficult problem as vehicular clusters change compositions dynamically and communities of interests are formed and dissolved rapidly. When multiple wireless access capabilities exist, it can complicate the problem of finding and addressing these dynamic network nodes. Sophisticated solutions can be developed that leverage the different capabilities of diverse networks for

the AHVN. Security and privacy continue to be a serious concern to users of wireless communications, particularly in the unlicensed bands. Efficient methods to transport multimedia data, especially video, over the AHVN will also need to be developed as vehicles become mobile nodes in the global network.

In this section, we outline some of the open issues and directions for future research to realize AHVN architecture and implement the corresponding protocols for vehicular telematics over heterogeneous wireless networks.

- *Enhanced multi-channel MAC protocols for DSRC*: Although the MAC for DSRC (i.e., IEEE 802.11p) follows the original IEEE 802.11 MAC and its extensions (e.g., IEEE 802.11e), the problem of multi-channel coordination/access in the DSRC MAC is open. This problem also needs to be addressed for a multihop V2V communication scenario. Efficient distributed multi-channel MAC protocols for DSRC can be developed based on the "cognitive radio" concept. A DSRC radio transceiver may use intelligent algorithms (e.g., reinforcement learning) to learn the surrounding environment and then to exploit the knowledge thus obtained to adaptively select the transmission channel and the transmission parameters (e.g., transmission power) to achieve the target system performance.
- *Dynamic spectrum sharing between DSRC and WiMAX radio*: For V2R communications through WiMAX base stations, dynamic spectrum sharing between DSRC radio and the WiMAX radio can potentially improve the communication efficiency as well as the spectrum utilization (and hence the service providers' revenue). This would be particularly true when the density of the vehicles (i.e., traffic load) increases, and therefore, the DSRC spectrum becomes congested. This dynamic spectrum sharing can be implemented through software-defined radio. Since dynamic spectrum access by multiple DSRC radio gives rise to a competitive scenario, game-theoretic models will be suitable to analyze this problem and the system dynamics.
- *Heterogeneous wireless access for vehicular telematics*: Efficient integration of different wireless access technologies (e.g., WiFi, WiMAX, 3G cellular) and optimal radio resource management for vehicular networks is an open problem. In the AHVN, resource management in multiple access networks should be addressed in order to maximize the resource utilization, robustness and stability of the network. Although still an open problem, some approaches could be the use of efficient system selection and handoff mechanisms along with dynamic spectrum sharing through software-defined radios. A related issue here is pricing of radio resources in the different access networks. A pricing model characterizes the service fee (i.e., price) for utilizing resources in a radio access network. To access the radio resources, a vehicular node has to pay to the radio resource owner which is typically the service provider. The decision on price setting has to be optimally made by a service provider (or radio resource owner) in a vehicular network to maximize network utility.
- *Multimedia transmission and QoS support over vehicular networks*: Multimedia (e.g., video) transmission in wireless environments is still a challenging task calling for high-compression efficiency as well as a network friendly design. Parameters in video coding, such as frame rate, quantization parameters, and frame dropping, can be controlled to give different bitrates (and hence different decoded video quality). There are challenges in adjusting these parameters in order to transmit multiple compressed video programs over wireless networks in real-time subject to channel fading, co-channel interference (CCI), and limited bandwidth and power [148]. Other factors are caused by mobility, network partitions and route failures, change in channel quality and data rate, and network load. Some of these have to be addressed by data congestion control at the same time.We need to understand its design limits due to its extreme bandwidth demands on real-time, and to provide adequate network resources from the limited bandwidth of the wireless network to support and differentiate the QoS requirements (e.g., reliability and latency) from different real-time streams. Previous wireless architecture and infrastructure are pretty much set up for either voice or data, which is not fit for transportation of video stream.
- *Data congestion in vehicular networks*: There is much work to extend its capability to wireless network especially if one wants to stay within the TCP realm in light of earlier discussion. The difficulties are the results of 1) dramatic changes in the BDP (Bandwidth-Delay Product) contributed by RTT (Round Trip Time) fluctuations, node mobility, and traffic load change at a mobile node, and 2) multihop communication characteristics in terms of path asymmetry, channel conditions from errors, medium contention, as well as hidden and exposed stations. To combat these problems several modifications to the transport layer were proposed in the literature. However, usefulness of these modifications needs to be investigated in a realistic V2R and V2V communications scenario considering lower layer protocol intricacies. Achieving a steady supply of bandwidth for streaming traffic in presence of congestion is a challenging task.
- *Cross-layer approaches*: Although the cross-layer approaches provide better performance, they are more complex to implement and design. Since implementation requires modification of multiple communication layers, joint optimization among all the layers can be challenging. Most of the works on the cross-layer optimization are derived from heuristics and simulation. A mathematical framework to characterize the interaction among the layers would be desirable. This would allow reliable algorithms to be developed for real-time applications which are becoming increasingly important for ITS applications over vehicular wireless networks.
- *Implementation of security* primitives with a good tradeoff between authentication, privacy, computational complexity, communication complexity and scalability in vehicular networks is a big research challenge. Some variation of the PKI system with careful trust analysis of OBU, RSU and authentication servers will eventually need to be adopted. Security primitives must be computationally lightweight for OBUs and should probably be derived from some suitable form of identity based cryptography, similar to one developed in [149,150]. RSUs should have tamper-free hardware as well (this is necessary for OBUs) and they should be connected using an IPSec tunnel [133] to the authentication server. Furthermore, all parties in the architecture should be able to authenticate each other. It is necessary to develop full protocols for transmission safety messages as well as protocols for transmission of liability messages during and after the accidents. These protocols should be developed for the scenarios where the infrastructure (RSUs and servers) is fully present, but also for the situations when only OBUs are present while the infrastructure is missing. Protocols for value added services (infotainment) and billing for all VANET services should be developed as well.
- Neither of the *privacy proposals* described before (with the exception of [135]) even mentions that OBU can be traced using its MAC address. An OBU can also be traced using its IP address, but since it is periodically changed via DHCP, the IP address traceability is more complex than MAC address traceability. Therefore, it is necessary to remove the source MAC address from the header of the MAC frame, and use some generic MAC address similarly to generic 0.0.0.0 IP address used in DHCP.
- At the application layer, there are challenges in *developing services and applications* for most effective use of ITS and data they collect. In particular, the implementation and software develop-

ment has to resemble and mirror that of similar complex infrastructures. The applications have to be as low level protocol agnostic as applications being developed for the web, capitalizing on the efficiencies of layered architectures and modern software engineering. Also, it is essential that applications scale up of any vehicular technology employed across a large number of vehicles that are intended to have more functionality than simple monitoring. Applications developed for next generation vehicular telematics will require an ITS-SOA similar to that in found in the business and electronic commerce sector. The new breed of ITS application developer will also need a healthy degree of statistical processing in his or her toolbox.

Acknowledgments

This work was supported by the AUTO21 NCE research grant for the project F303-FVT. The authors would like to thank Khajonpong Akkarajitsakul, Subir Biswas, Man Hon Cheung, Mahbubul Haque, Kelly He, Yang Hong, Seyed Ali Hosseininezhad, Jinwoo Lee, Brijech K. Mohandas, Kaveh Shafiee, Joo-Han Song, and Daxin Tian for their contributions towards this article.

References

[1] W. Chen, S. Cai, Ad hoc peer-to-peer network architecture for vehicle safety communications, IEEE Communications Magazine 43 (4) (2005) 100–107. April.
[2] S. Biswas, R. Tatchikou, F. Dion, Vehicle-to-vehicle wireless communication protocols for enhancing highway traffic safety, IEEE Communications Magazine 44 (1) (2006) 74–82. January.
[3] M. Wellens, B. Westphal, P. Mahonen, Performance evaluation of IEEE 802.11-based WLANs in vehicular scenarios, in: Proceedings of IEEE Vehicular Technology Conference (VTC) Spring, April 2007, pp. 1167–1171.
[4] J. Luo, J.-P. Hubaux, A survey of inter-vehicle communication, EPFL Technical Report IC/2004/24, March 2004.
[5] D. Gray (Ed.), Mobile WiMAX Part I: A Technical Overview and Performance Evaluation v2.8, Apr 2006, http://www.wimaxforum.org/techno-Logy/downloads/Mobile_WiMAX_Part1_Overview_and_Performance.pdf, last access by July, 2007.
[6] D. Jiang, L. Delgrossi, IEEE 802.11p: towards an international standard for wireless access in vehicular environments, in: Proceedings of IEEE Vehicular Technology Conference (VTC) Spring, May 2008, pp. 2036–2040.
[7] K. Yang, S. Ou, H.-H. Chen, J. He, A multihop peer-communication protocol with fairness guarantee for IEEE 802.16-based vehicular networks, IEEE Transactions on Vehicular Technology 56 (6) (2007) 3358–3370. Part 1, November.
[8] H. Menouar, F. Filali, M. Lenardi, A survey and qualitative analysis of MAC protocols for vehicular ad hoc networks, IEEE Wireless Communications 13 (5) (2006) 30–35. October.
[9] M. Khabazian, M. Ali, A performance modeling of connectivity in vehicular ad hoc networks, IEEE Transactions on Vehicular Technology 57 (4) (2008) 2440–2450. July.
[10] F. Xie, K.A. Hua, W. Wang, Y.H. Ho, Performance study of live video streaming over highway vehicular ad hoc networks, in: Proceedings of IEEE Vehicular Technology Conference (VTC) Spring 2007, September–October 2007, pp. 2121–2125.
[11] <http://www.cvisproject.org/>.
[12] <http://www.sevecom.org/>.
[13] <http://www.preciosa-project.org/>.
[14] <http://evita-project.org/>.
[15] <http://www.com2react-project.org/>.
[16] <http://www.ertico.com>.
[17] <http://wiki.fot-net.eu/index.php?title=SIM-TD>.
[18] <http://www.safespot-eu.org/>.
[19] <http://www.comesafety.org/>.
[20] <http://www.geonet-project.eu/>.
[21] CarTalk2000, <http://www.cartalk2000.net>.
[22] FleetNet Program, 2001. <http://www.fleetnet.de>.
[23] L. Stranden, E. Uhlemann, E.G. Strom, State of the art survey of wireless vehicular communication projects, in: Proceedings of 15th World Congress on Intelligent Transport Systems (ITS), New York City, NY, November 2008.
[24] G. Korkmaz, E. Ekici, F. Ozguner, Urban multihop broadcast protocols for inter-vehicle communication systems, in: Proceedings of First ACM Workshop on Vehicular Ad-hoc Networks (VANET'04), October 2004, pp. 76–85.
[25] J. Zhao, Y. Zhang, G. Cao, Data pouring and buffering on the road: a new data dissemination paradigm for vehicular ad hoc networks, IEEE Transactions on Vehicular Technology 56 (6) (2007) 3266–3277. November.
[26] G. Kokmaz, E. Ekici, F. Ozguner, Black-burst-based multihop broadcast protocols for vehicular networks, IEEE Transactions on Vehicular Technology 56 (5) (2007) 3159–3167. September.
[27] K. Shafiee, V.C.M. Leung, A reliable robust fully ad hoc data dissemination mechanism for vehicular network, International Journal of Advanced Science and Technology 2 (2009) 53–62. January.
[28] L. Wischhof, A. Ebner, H. Rohling, M. Lott, R. Halfmann, SOTIS: a self-organizing traffic information system, in: Proceedings of IEEE Vehicular Technology Conference, April 2003, pp. 2442–2446.
[29] T. Nadeem, S. Dashtinezhad, C. Liao, L. Iftode, TrafficView: traffic data dissemination using car-to-car communication, ACM SIGMOBILE Mobile Computing and Communications Review 8 (3) (2004) 6–19. July.
[30] L. Wischhof, A. Ebner, H. Rohling, Information dissemination in self-organizing intervehicle networks, IEEE Transactions on Intelligent Transportation Systems 6 (1) (2005) 90–101. March.
[31] B.S. Kerner, C. Demir, R.G. Herrtwich, S.L. Klenov, H. Rehborn, M. Aleksic, A. Haug, Traffic state detection with floating car data in road networks, in: Proceedings of the 8th International IEEE Conference on Intelligent Transportation Systems, September 2005, pp. 44–49.
[32] G. Halbritter, T. Fleischer, C. Kupsch, J. Kloas, U. Voigt, Nationale Innovationsstrategien fr neue Techniken und Dienste zur Erreichung einer nachhaltigen Entwicklung im Verkehr, DIW Berlin, Report FZKA 7157, Forschungszentrum Karlsruhe GmbH, Karlsruhe, 2005.
[33] A. Brzezinski, G. Zussman, Enabling distributed throughput maximization in wireless mesh networks – a partitioning approach, in: Proceedings of ACM MOBICOM'06, September 2006, pp. 26–37.
[34] V. Bychkovsky, B. Hull, A. Miu, H. Balakrishnan, S. Madden, A measurement study of vehicular Internet access using unplanned 802.11 networks, in: Proceedings of ACM MOBICOM'06, September 2006.
[35] J. Ott, D. Kutscher, Drive-thru Internet: IEEE 802.11b for automobile users, in: Proceedings of IEEE INFOCOM, March 2004.
[36] R. Gass, J. Scott, C. Diot, Measurements of in-motion 802.11 networking, in: Proceedings of IEEE Workshop on Mobile Computing Systems and Applications, August 2005, pp. 69–74.
[37] M.L. Sim, M. Nekovee, Y.F. Ko, Throughput analysis of Wi–Fi based broadband access for mobile users on the highway, in: Proceedings of Joint IEEE Malaysia International Conference on Communications and IEEE International Conference on Network (MICC & ICON), p. 6, November 2005.
[38] S.R. Dickey, C.-L. Huang, X. Guan, Field measurements of vehicle to roadside communication performance, in: Proceedings of IEEE Vehicular Technology Conference (VTC) Fall, September–October 2007, pp. 2179–2183.
[39] H. Cai, Y. Lin, Design of a roadside seamless wireless communication system for intelligent highway, in: Proceedings of IEEE Networking, Sensing and Control, March 2005, pp. 342–347.
[40] L. Wischhof, A. Ebner, H. Rohling, M. Lott, R. Halfmann, Adaptive broadcast for travel and traffic information distribution based on inter-vehicle communication, in: Proceedings of IEEE Intelligent Vehicles Symposium, June 2003, pp. 6–11.
[41] D.G. Oh, P. Kim, Y.J. Song, S.I. Jeon, H.J. Lee, Design considerations of satellite-based vehicular broadband networks, IEEE Communications Magazine 12 (5) (2005) 91–97. October.
[42] S. Pack, H. Rutagemwa, X. Shen, J. Mark, K. Park, Efficient data access algorithms for ITS-based networks with multihop wireless links, in: Proceedings of IEEE International Conference on Communications (ICC) 2007, June 2007, pp. 4785–4790.
[43] S. Yousefi, M.S. Mousavi, M. Fathy, Integrated architecture for message dissemination in vehicular ad hoc networks, in: Proceedings of 6th International Conference on ITS Telecommunications, June 2006, pp. 57–60.
[44] Y.F. Ko, M.L. Sim, M. Nekovee, Wi–Fi based broadband wireless access for users on the road, BT Technology Journal 24 (2) (2006) 123–129. April.
[45] C.C. Hung, H. Chan, E.H.K. Wu, Mobility pattern aware routing for heterogeneous vehicular networks, in: Proceedings of IEEE Wireless Communications and Networking Conference (WCNC), March–April 2008, pp. 2200–2205.
[46] I.F. Akyildiz, S. Mohanty, J. Xie, A ubiquitous mobile communication architecture for next-generation heterogeneous wireless systems, IEEE Communications Magazine 43 (6) (2005) S29–S36. June.
[47] D. Johnson, C. Perkins, J. Arkko, RFC 3775: Mobility support in IPv6, IETF, June 2004.
[48] F. Bari, V.C.M. Leung, Automated network selection in a heterogeneous wireless network environment, IEEE Network 21 (1) (2007) 34–40. January.
[49] J. Xie, I.F. Akyildiz, A hybrid control resource allocation scheme for policy-enabled handoff in wireless heterogeneous overlay networks, 2004.
[50] D. Niyato, E. Hossain, Dynamics of network selection in heterogeneous wireless networks: an evolutionary game approach, IEEE Transactions on Vehicular Technology 58 (4) (2009) 2008–2017. May.
[51] O. Ormond, J. Murphy, G.-M. Muntean, Utility-based intelligent network selection in beyond 3G systems, in: Proceedings of IEEE International Conference on Communications (ICC), vol. 4, June 2006, pp. 1831–1836.
[52] O. Sallent, J. Perez-Romero, R. Agusti, L. Giupponi, C. Kloeck, I. Martoyo, S. Klett, J. Luo, Resource auctioning mechanisms in heterogeneous wireless access networks, in: Proceedings of IEEE Vehicular Technology Conference (VTC) Spring, vol. 1, May 2006, pp. 52–56.
[53] N. Shenoy, R. Montalvo, A framework for seamless roaming across cellular and wireless local area networks, IEEE Wireless Communications 12 (3) (2005) 50–57. June.

[54] V. Gazis, N. Alonistioti, L. Merakos, Toward a generic always best connected capability in integrated WLAN/UMTS cellular mobile networks (and beyond), IEEE Wireless Communications 12 (3) (2005) 20–29. June.
[55] D. Sanders, M. Laskowski, R.D. McLeod, A framework for mobile wireless applications, Presented at WIN-ITS, Vancouver, August 2007.
[56] Reference Model for Service Oriented Architecture 1.0 OASIS Standard, <http://docs.oasis-open.org/soa-rm/v1.0/>, October 2006 (accessed October 2008).
[57] O. Maeshima, S. Cai, T. Honda, H. Urayama, A roadside-to-vehicle communication system for vehicle safety using dual frequency channels, in: Proceedings of IEEE Intelligent Transportation Systems Conference (ITSC) 2007, September–October 2007, pp. 349–354.
[58] C.-J. Chang, R.-G. Cheng, H.-T. Shih, Y.-S. Chen, Maximum freedom last scheduling algorithm for downlinks of DSRC networks, IEEE Transactions on Intelligent Transportation Systems 8 (2) (2007) 223–232. June.
[59] Y. Yang, M. Marina, R. Bagrodia, Evaluation of multihop relaying for robust vehicular Internet access, in: Proceedings of IEEE 2007 Mobile Networking for Vehicular Environments, May 2007, pp. 19–24.
[60] H. Su, X. Zhang, Clustering-based multichannel MAC protocols for QoS provisionings over vehicular ad hoc networks, IEEE Transactions on Vehicular Technology 56 (6) (2007) 3309–3323. November.
[61] B. Sikdar, Design and analysis of a MAC protocol for vehicle to roadside networks, in: Proceedings of IEEE Wireless Communications and Networking Conference (WCNC), March–April 2008, pp. 1691–1696.
[62] J. Zhang, Q. Zhang, W. Jia, A novel MAC protocol for cooperative downloading in vehicular networks, in: Proceedings of IEEE Global Telecommunications Conference (GLOBECOM'07), November 2007, pp. 4974–4978.
[63] J. Zhu, S. Roy, MAC for dedicated short range communications in intelligent transport system, IEEE Communications Magazine 41 (12) (2003) 60–67. December.
[64] Y. Zhang, J. Zhao, G. Cao, On scheduling vehicle-roadside data access, in: Proceedings of the fourth ACM international workshop on Vehicular ad hoc networks, September 2007, pp. 9–18.
[65] W. Xing, X.H. Nguyen, Y. Li, WiMAX fast-moving access network, in: Proceedings of IEEE Wireless Communications and Networking Conference(WCNC), March–April 2008, pp. 2663–2668.
[66] D. Jiang, V. Taliwal, A. Meier, W. Holfelder, R. Herrtwich, Design of 5.9 GHz DSRC-based vehicular safety communication, IEEE Wireless Communications 13 (5) (2006) 36–43. October.
[67] Y. Mertens, M. Wellens, P. Mahonen, Simulation-based performance evaluation of enhanced broadcast schemes for IEEE 802.11-based vehicular networks, in: Proceedings of IEEE Vehicular Technology Conference (VTC) Spring, May 2008, pp. 3042–3046.
[68] O.K. Tonguz, N. Wisitpongphan , F. Bai, P. Mudalige, V. Sadekar, Broadcasting in VANET, in: Proceedings of IEEE INFOCOM MOVE Workshop 2007, May 2007, pp. 7–12.
[69] N. Wisitpongphan, O.K. Tonguz, J.S. Parikh, P. Mudalige, F. Bai, V. Sadekar, Broadcast storm mitigation techniques in vehicular ad hoc wireless networks, IEEE Wireless Communications 14 (6) (2007) 84–94. December.
[70] S. Ni, Y. Tseng, Y. Chen, J. Sheu, The broadcast storm problem in a mobile ad hoc network, in: Proceedings of ACM Mobicom, 1999, pp. 151–162.
[71] M. Caliskan, D. Graupner, M. Mauve, Decentralized discovery of free parking places, in: Proceedings of the 3rd ACM International Workshop on Vehicular Ad Hoc Networks, September 2006, pp. 30–39.
[72] C. Lochert, B. Scheuermann, M. Mauve, Probabilistic aggregation for data dissemination in VANETs, in: Proceedings of ACM VANET, September 2007, pp. 1–8.
[73] J. Chennikara-Varghese, W. Chen, O. Altintas, S. Cai, Survey of routing protocols for inter-vehicle communications, in: Proceedings of 3rd Annual International Conference on Mobile and Ubiquitous Systems – Workshops, pp. 1–5, 17–21 July 2006, San Jose, CA, USA, Digital Object Identifier 10.1109/MOBIQW.2006.361764.
[74] O. Abedi, M. Fathy, J. Taghiloo, Enhancing AODV routing protocol using mobility parameters in VANET, in: Proceedings of IEEE/ACS International Conference on Computer Systems and Applications (AICCSA 2008), March–April 2008, pp. 229–235.
[75] V. Naumov, R. Baumann, T. Gross, An evaluation of inter-vehicle ad hoc networks based on realistic vehicular traces, in: Proceedings of ACM MobiHoc, May 2006, pp. 108–119.
[76] Z. Mo, H. Zhu, K. Makki, N. Pissinou, MURU: a multihop routing protocol for urban vehicular ad hoc networks, in: Proceedings of the 3rd Annual International Conference on Mobile and Ubiquitous Systems: Networks and Services (MOBIQUITOUS), July 2006, pp. 1–8.
[77] H.F. Wedde, S. Lehnhoff, B.V. Bonn, Highly dynamic and scalable VANET routing for avoiding traffic congestions, in: Proceedings of the Fourth ACM International Workshop on Vehicular Ad hoc Networks, September 2007, pp. 81–82.
[78] T. Taleb, E. Sakhaee, A. Jamalipour, K. Hashimoto, N. Kato, Y. Nemoto, A stable routing protocol to support ITS services in VANET networks, IEEE Transactions on Vehicular Technology 56 (6) (2007) 3337–3347. November.
[79] J. Tian, L. Han, K. Rothermel, C. Cseh, Spatially aware packet routing for mobile ad hoc inter-vehicle radio networks, in: Proceedings of ITS'03, October 2003, pp. 1546–1551.
[80] B. Seet, G. Liu, B. Lee, C. Foh, K. Wong, K. Lee, A-STAR: a mobile ad hoc routing strategy for metropolis vehicular communications, Lecture Notes in Computer Science 3042 (0302-9743) (2004) 989–999. January.
[81] J. Zhao, G. Cao, VADD: vehicle-assisted data delivery in vehicular ad hoc networks, in: Proceedings of IEEE INFOCOM'06, April 2006, pp. 1–12.
[82] V. Naumov, T.R. Gross, Connectivity-aware routing (CAR) in vehicular ad hoc networks, in: Proceedings of IEEE INFOCOM'07, May 2007, pp. 1919–1927.
[83] N. Wisitpongphan, F. Bai, P. Mudalige, V. Sadekar, O. Tonguz, Routing in sparse vehicular ad hoc wireless networks, IEEE Journal on Selected Areas in Communications 25 (8) (2007) 1538–1556. October.
[84] V. Namboordiri, L. Gao, Prediction-based routing for vehicular ad hoc networks, IEEE Transactions on Vehicular Technology 56 (4) (2007) 2332–2345. July.
[85] R. He, H. Rutagemwa, X. Shen, Differentiated reliable routing in hybrid vehicular ad-hoc networks, in: Proceedings of IEEE ICC'08, May 2008, pp. 2353–2358.
[86] H. Balakrishnan, V.N. Padmanabhan, S. Seshan, R.H. Katz, A comparison of mechanisms for improving TCP performance over wireless links, IEEE/ACM Transactions on Networking 5 (6) (1997) 756–769. December.
[87] Z. Fu, H. Luo, P. Zerfos, S. Lu, L. Zhang, M. Gerla, The impact of multihop wireless channel on TCP performance, IEEE Transactions on Mobile Computing 4 (2) (2005) 209–221. March–April.
[88] V. Jacobson, M.J. Karels, Congestion avoidance and control, in: Proceedings of ACM SIGCOMM '88 Workshop, 1988, pp. 314–329.
[90] Y. Zang, L. Stibor, X. Cheng, H. Reumerman, A. Paruzel, A. Barros, Congestion control in wireless networks for vehicular safety applications, in: Proceedings of 13th European Wireless Conference, April 2007.
[91] J. Mo, J. Walrand, Fair end-to-end window-based congestion control, IEEE/ACM Transactions on Networking 8 (5) (2000) 556–567. October.
[92] L. Zhao, Y. Jing, G.M. Dimirovski, Improvement of AIMD algorithm considering multimedia transfer over Internet, in: Proceedings of the 6th International Conference on Telecommunications in Modern Satellite, Cable and Broadcasting Service, October 2003, pp. 392–394.
[93] C. Huang, L. Xu, SRC: Stable rate control for streaming media, in: Proceedings of IEEE Globecom, December 2003, pp. 4016–4021.
[94] W.R. Stevens, TCP slow start, congestion avoidance, fast retransmit and fast recovery algorithms, IETF RFC 2001, September 1997.
[95] G. Hasegawa, M. Murata, H. Miyahara, Fairness and stability of congestion control mechanisms of TCP, in: Proceedings of INFOCOM'99, March 1999, pp. 1329–1336.
[96] S. Floyd, T. Henderson, The NewReno modification to TCP's fast recovery algorithm, IETF RFC 2582, April 1999.
[97] S. Kim, S. Choi, C. Kim, Instantaneous variant of TCP NewReno, Electronics Letters, October 1999, pp. 1818–1820.
[98] N. Parvez, A. Mahanti, C. Williamson, TCP NewReno: slow-but-steady or impatient?, in: Proceedings of IEEE International Conference on Communications (ICC'06), June 2006, pp. 716–722.
[99] S. Floyd, V. Jacobson, Random early detection gateways for congestion avoidance, IEEE/ACM Transactions on Networking 1 (4) (1993) 397–413. August.
[100] M. May, J. Bolot, C. Diot, B. Lyles, Reasons not to deploy RED, in: Proceedings of the 7th International Workshop on Quality of Service, IWQoS, June 1999, pp. 260–262.
[101] S. Floyd, R. Gummadi, S. Shenker, Adaptive RED: an algorithm for increasing the robustness of RED, UC Berkeley ICIR Technical Report, August 2001, <http://www.icir.org/floyd/papers/adaptiveRed.pdf>.
[102] K. Xu, M. Gerla, L. Qi, Y. Shu, Enhancing TCP fairness in ad-hoc wireless networks using neighborhood RED, in: Proceedings of ACM 9th Annual International Conference on Mobile Computing and Networking (Mobicom 2003), September 2003, pp. 16–28.
[103] W. Feng, K. Shin, D. Kandlur, D. Saha, The blue: active queue management algorithms, IEEE/ACM Transactions on Networking 10 (4) (2002) 513–528. August.
[104] D. Lin, R. Morris, Dynamics of random early detection, in: Proceedings of Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication, 1997, pp. 127–137.
[106] S. Kunniyur, R. Srikant, An adaptive virtual queue (AVQ) algorithms for active queue management, IEEE/ACM Transactions on Networking 12 (2) (2004) 286–299. April.
[108] M. Hanley, S. Floyd, J. Padhye, J. Widmer, TCP Friendly Rate Control (TFRC): Protocol Specification, IETF RFC 3448, January 2003.
[109] D. Katabi, M. Handley, C. Rohrs, Congestion control for high bandwidth delay product networks, in: Proceedings of ACM SIGCOMM'02, October 2002, pp. 89–102.
[110] K. Chen, K. Nahrstedt, and N. Vaidya, The utility of explicit rate-based flow control in mobile ad-hoc networks, in: Proceedings of IEEE Wireless Communication and Networking Conference, vol. 3, March 2004, pp. 1921–1926.
[111] Y. Hong, O.W.W. Yang, Design of adaptive PI rate controller for best-effort traffic in the Internet based on phase margin, IEEE Transactions on Parallel and Distributed Systems 18 (4) (2007) 550–561. April.
[112] L. Wischhof, H. Rohling, Congestion control in vehicular ad hoc networks, in: Proceedings of IEEE International Conference on Vehicular Electronics and Safety 2005 (ICVES 2005), October 2005, pp. 58–63.
[113] S. Shakkottai, T.S. Rappaport, P.C. Karlsson, Cross-layer design for wireless networks, IEEE Communications Magazine 41 (10) (2003) 74–80. October.
[114] M. Chiang, To layer or not to layer: balancing transport and physical layers in wireless multihop networks, in: Proceedings of IEEE INFOCOM'04, April 2004, pp. 2525–2536.

[115] L. Bononi, M. Di Felice, A cross layered MAC and clustering scheme for efficient broadcast in VANETs, in: Proceedings of 1st IEEE International Workshop on Mobile Vehicular Networks (MoVeNet), 2007.
[116] X. Xie, F. Wang, H. Wang, K. Li, Adaptive multi-channel MAC protocol for dense VANET using directional antennas, in: Proceedings of Second International Conference on Future Generation Communication and Networking, vol. 2, 2008, pp. 398–401.
[117] C. Cuyu, X. Yong, S. Meilin, L. Liang, Performance observations on MAC protocols of VANETs in intelligent transportation system, in: Proceedings of International Conference on Communications and Mobile Computing, vol. 2, 2009, pp. 373–379.
[118] J.-H. Song, V.W.S. Wong, V.C.M. Leung, Wireless location privacy protection in vehicular ad-hoc networks, ACM/Springer Mobile Networks and Applications (MONET), in press, doi:10.1007/s11036-009-0167-4.
[119] J.-H. Song, V.W.S. Wong, V.C.M. Leung, Secure location verification for vehicular ad-hoc networks, in: Proceedings of IEEE Global Communications Conference (Globecom), New Orleans, LA, November/December 2008.
[120] M. Raya, J.-P. Hubaux, The security of vehicular ad hoc networks, in: Proceedings of 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks 2005, 2005, pp. 11–21.
[121] B. Parno, A. Perrig, Challenges in securing vehicular networks, in: Proceedings of Workshop on Hot Topics in Networks (HotNets-IV), 2005.
[122] E. Coronado, S. Cherkaoui, An AAA study for service provisioning in vehicular networks, in: Proceedings of 32nd IEEE Conference on Local Computer Networks 2007, October 2007, pp. 669–676.
[123] X. Sun, X. Lin, P.H. Ho, Secure vehicular communications based on group signature and id-based signature scheme, in: Proceedings of International Conference on Communications 2007 (ICC'07), June 2007, pp. 1539–1545.
[124] M. Raya, J.-P. Hubaux, Securing vehicular ad hoc networks, Journal of Computer Security 15 (2007) 39–68. IOS Press.
[125] A. Aijaz, B. Bochow, F. Doetzer, A. Festag, M. Gerlach, R. Kroh, T. Leimueller, Attacks on inter vehicle communication systems – an analysis, in: Proceedings of 3rd International Workshop on Intelligent Transportation (WIT 2006), 14–15 March, 2006.
[126] M. Raya, A. Aziz, J.-P. Hubaux, Efficient secure aggregation in VANETs, in: Proceedings of 3rd International Workshop on Vehicular Ad hoc Networks, Los Angeles, CA, USA, 2006, pp. 67–75.
[127] F. Picconi, N. Ravi, M. Gruteser, L. Iftode, Probabilistic validation of aggregated data in vehicular ad-hoc networks, in: Proceedings of 3rd International Workshop on Vehicular Ad hoc Networks, Los Angeles, CA, USA, 2006, pp. 76–85.
[128] T. Leinmueller, C. Maihoefer, E. Schoch, F. Kargl, Improved security in geographic ad-hoc routing through autonomous position verification, in: Proceedings of 3rd International Workshop on Vehicular Ad hoc Networks, Los Angeles, CA, USA, 2006, pp. 57–66.
[129] P. Golle, D. Greene, J. Staddon, Detecting and correcting malicious data in VANETs, in: Proceedings of 1st ACM international Workshop on Vehicular Ad hoc Networks, Philadelphia, PA, USA, 2004, pp. 29–37.
[130] M. El Zarki, S. Mehrotra, N. Tsudik, N. Venkatasubramanian, Security issues in future vehicular network, in: Proceedings of European Wireless Conference 2002, 2002.
[131] J. Blum, A. Eskandarian, The threat of intelligent collisions, IEEE IT Professional Magazine, January–February 2004, pp. 24–29.
[132] Vehicle Safety Communications Project – Final report, U.S. Department of Transportation, National Highway Safety Administration, 2006, <http://www-nrd.nhtsa.dot.gov/pdf/nrd-12/060419-0843/PDFTOC.htm>.
[133] M. Bishop, Computer Security: Art and Science, Pearson Education, Inc., Boston, MA 02116, 1st edition, 2003.
[134] X. Lin, X. Sun, P. Ho, X. Shen, GSIS: a secure and privacy-preserving protocol for vehicular communications, IEEE Transactions on Vehicular Technology 56 (6) (2007) 3442–3456. November.
[135] L. Buttyan, J.-P. Hubaux, F. Kargl, M. Raya, Architecture for secure and private vehicular communications, in: Proceedings of ITST 2007, June 2007.
[136] D. Chaum, Security without identification: transactions to make big brother obsolete, Communication of the ACM 28 (10) (1985) 1030–1044.
[137] J. Choi, M. Jakobsson, S.Wetzel, Balancing auditability and privacy in vehicular networks, in: Proceedings of Q2SWinet 2005, 2005, pp. 79–87.
[138] K. Plossl, T. Nowey, C. Mletzko, Towards a security architecture for vehicular ad hoc networks, in: Proceedings of the First International Conference on Availability, Reliability and Security ARES 2006, April 2006, p. 8.
[139] H. Moustafa, G. Bourddon, Y. Gourhant, Providing authentication and access control on vehicular environments, in: Proceedings of IFIP 2006, 2006, pp. 62–73.
[140] K. Sha, Y. Xi, W. Shi, L. Schwiebert, T. Zhang, Adaptive privacy-preserving authentication in vehicular networks, in: Proceedings of First International Conference on Communications and Networking in China, October 2006, pp. 1–8.
[141] Y. Xi, K. Sha, W. Shi, L. Schwiebert, T. Zhang, Enforcing privacy using symmetric random key-set in vehicular networks, in: Proceedings of Eighth International Symposium on Autonomous Decentralized Systems (ISADS'07), March 2007, pp. 344–351.
[142] A. Perrig, R. Canneti, D. Tygar, D. Song, The tesla broadcast authentication protocol, RSA Cryptobytes 5 (2) (2002) 2–13.
[143] X. Lin, C. Zhang, X. Sun, P.-H. Ho, X. Shen, Performance enhancement for secure vehicular communications, in: Proceedings of IEEE Global Communications Conference (GLOBECOM'07), Washington, DC, USA, Nov. 26–30, 2007.
[144] L. Lamport, Password authentication with insecure communication, Communication of the ACM 24 (11) (1981) 770–772.
[145] S. Capkun, J.-P. Hubaux, M. Jakobsson, Secure and privacy preserving communications in hybrid ad hoc networks, Technical Report EPFL-IC, EPFL, 2004.
[146] F. Dotzer, Privacy issues in VANET, in: Proceedings of Workshop on Privacy Enhancing Technologies, 2005.
[147] K. Sampigethaya, L. Huang, M. Li, R. Poovendran, K. Matsura, K. Sezaki, Caravan: Providing location privacy for VANET, in: Proceedings of Workshop on Embedded Security in Cars, 2005.
[148] G.-M. Su, Z. Man, M. Wu, K.J.R. Liu, Multiuser cross-layer resource allocation for video transmission over wireless networks, IEEE Network 20 (2) (2006) 21–27. March–April.
[149] K. Ren, W. Lou, K. Kim, R. Deng, A novel privacy preserving authentication and access control scheme for pervasive computing environments, IEEE Transactions on Vehicular Technology 55 (4) (2006) 1373–1384. July.
[150] S. Wang, Anonymous wireless authentication on a portable cellular mobile system, IEEE Transactions on Computers 53 (10) (2004) 1317–1329. October.