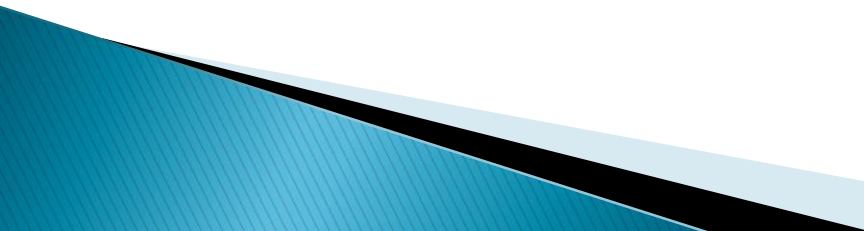


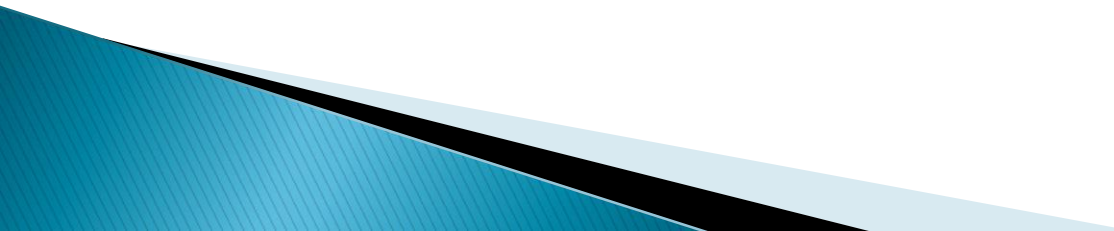
Vehicular Ad-Hoc Networks (VANET)



Motivation

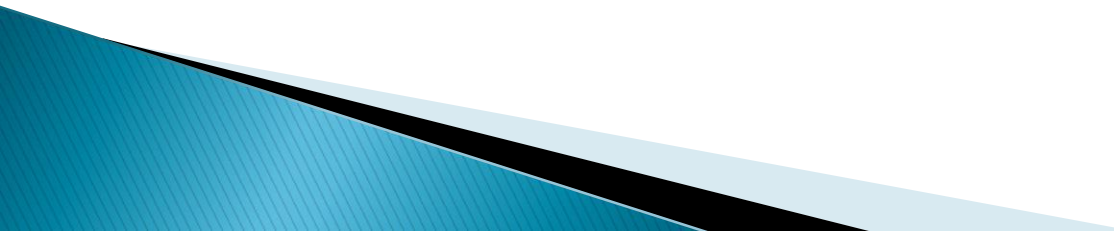
- ▶ Safety and transport efficiency
 - Congestion costs the U.S. economy over \$100 billion per year by 2022.
 - Vehicle occupancy has dropped 7% in the last two decades.
 - In Europe around 40,000 people die and more than 1.5 millions are injured every year on the roads
 - Traffic jams generate a tremendous waste of time and of fuel
- 

Definition

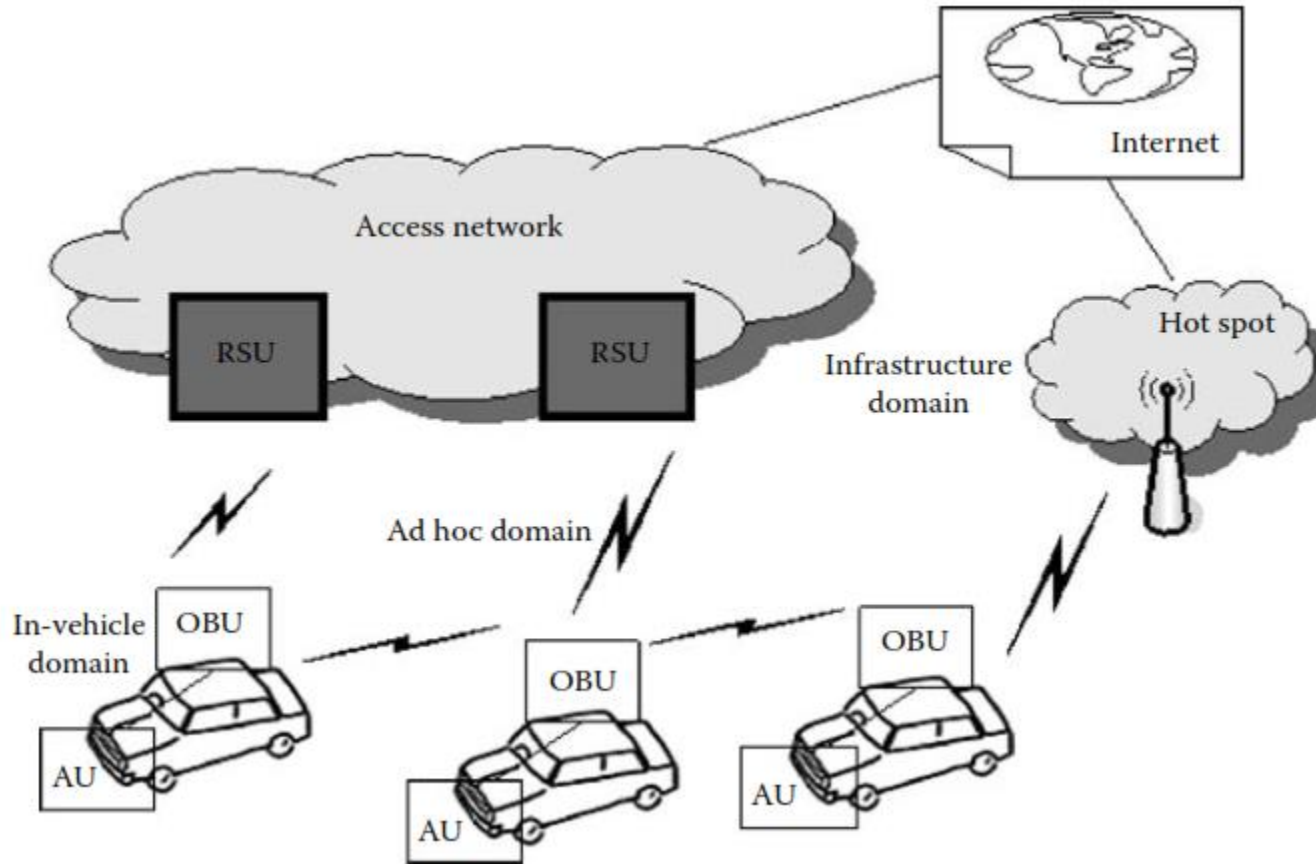
- ▶ Vehicular networks are a novel class of wireless networks that have emerged thanks to advances in wireless technologies and the automotive industry.
 - ▶ These networks, also known as VANETs, are considered as one of the ad hoc network real-life applications, enabling communications among nearby vehicles as well as between vehicles and nearby fixed equipment, usually described as roadside equipment.
 - ▶ .
- 

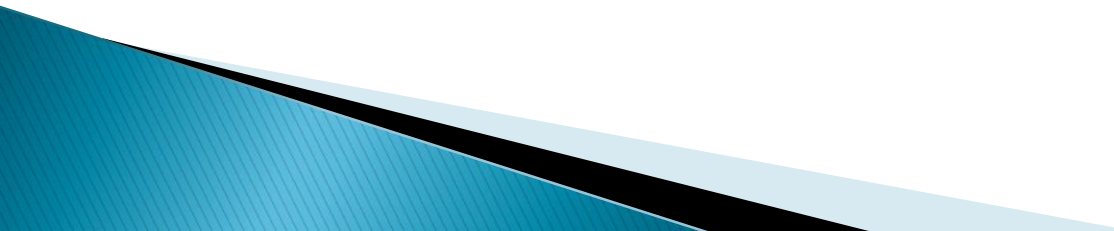
- ▶ Dedicated short-range communications (DSRC) system has emerged.
 - ▶ Car-to Car Communication Consortium (C2C-CC) has been initiated in Europe by car manufacturers and automotive OEMs.
 - ▶ IEEE is also advancing within the IEEE 1609 family of standards for wireless access in vehicular environments (WAVE).
- 

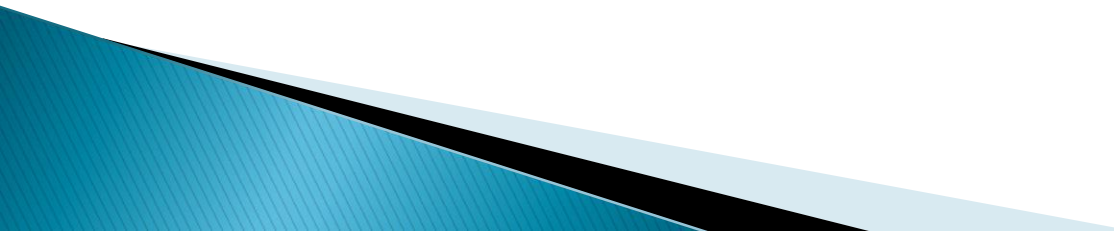
Architecture

- ▶ a pure wireless vehicle-to-vehicle adhoc network (V2V) allowing standalone vehicular communication with no infrastructure support,
 - ▶ (ii) a wired backbone with wireless last hops that can be seen as a WLAN-like vehicular network,
 - ▶ (iii) and a hybrid vehicle-to-road (V2R) architecture that does not rely on a fixed infrastructure in a constant manner
- 

C2C-CC Architecture

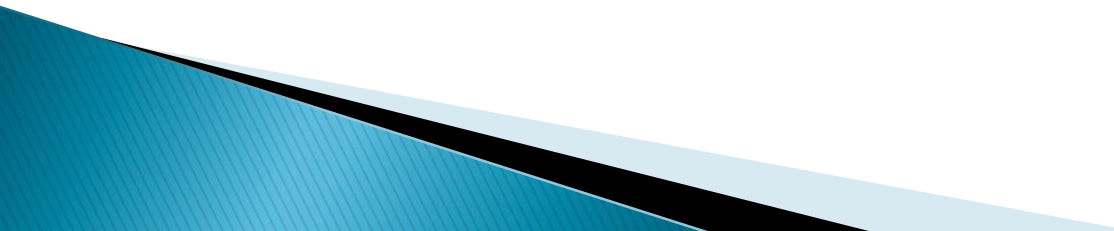


- ▶ An OBU is a device in the vehicle having communication capabilities (wireless and/or wired),
 - ▶ AU is a device executing a single or a set of applications while making use of the OBU's communication capabilities. laptop or PDA
 - ▶ AU and OBU Bluetooth
 - ▶ Roadside units (RSUs) that are stationary along the road
- 

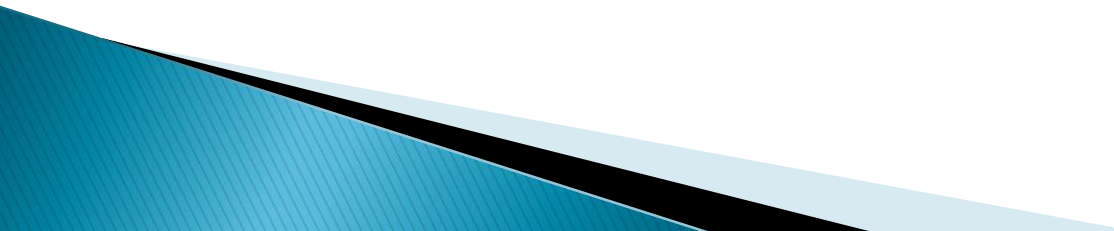
- ▶ Unlimited transmission power: Mobile device power issues are usually not a significant constraint in vehicular networks.
 - ▶ Higher computational capability: Indeed, operating vehicles can afford significant computing, communication, and sensing capabilities.
 - ▶ Predictable mobility: Unlike classic mobile ad hoc networks, where it is hard to predict the nodes' mobility.
- 

- ▶ Potentially large scale:
- ▶ High mobility
- ▶ Partitioned network
- ▶ Network topology and connectivity: dynamic

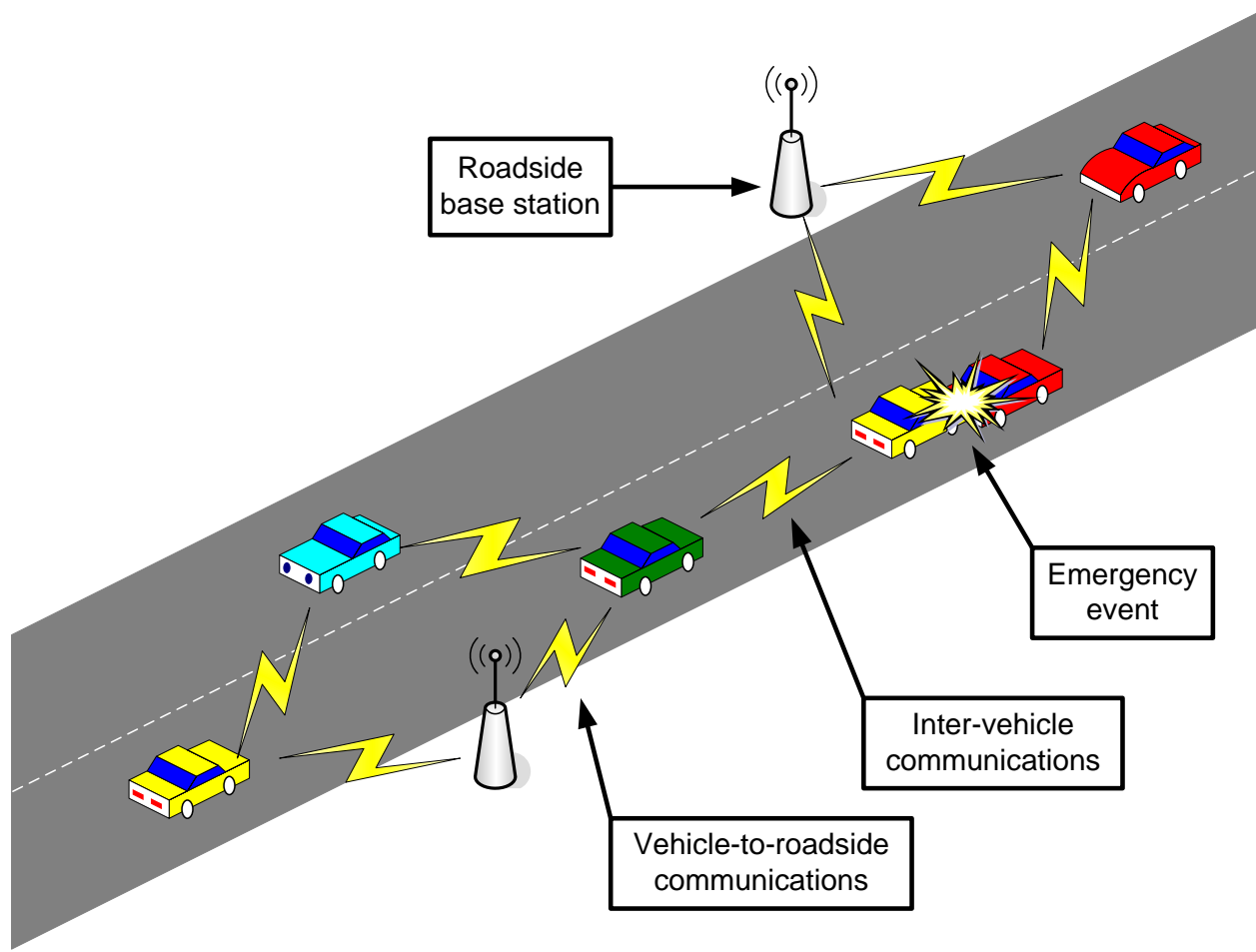
Ad-Hoc Network

- ▶ A network with minimal or no infrastructure
 - ▶ It is a temporary network composed of mobile terminals fitted with a relay function.
 - ▶ Self-organizing
 - ▶ Mobile nodes act as network router
mobile nodes provides not only function for information transmission and reception but also function for information relay.
- 

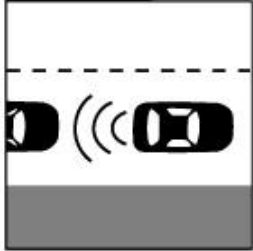
Vehicular Ad-Hoc Networks

- ▶ It is special form of MANET and it provides
 - Vehicle-to-vehicle communications
 - Vehicle-to-infrastructure communications
 - ▶ Uses equipped vehicles as the network nodes
 - ▶ Nodes move at will relative to each other but within the constraints of the road infrastructure
- 

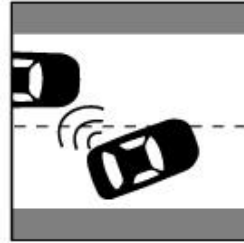
Vehicular Ad-Hoc Networks (Example)



VANET Applications



Co-operative Collision Warning



Lane Change Warning



Intersection Collision Warning



Approaching Emergency vehicle



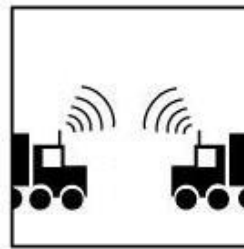
Rollover Warning



Work Zone Warning



Coupling/Decoupling

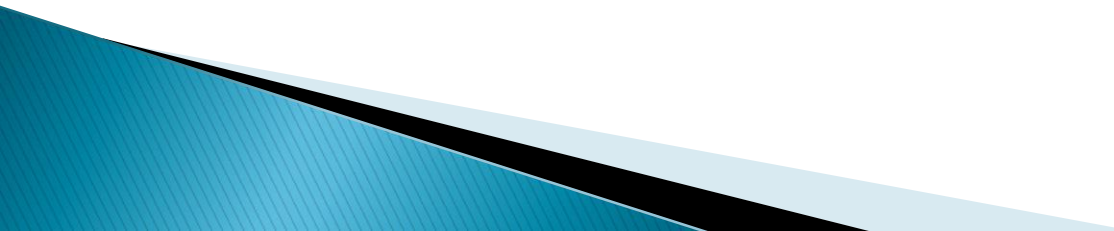


Inter-Vehicle Communications



Electronic Toll Collection

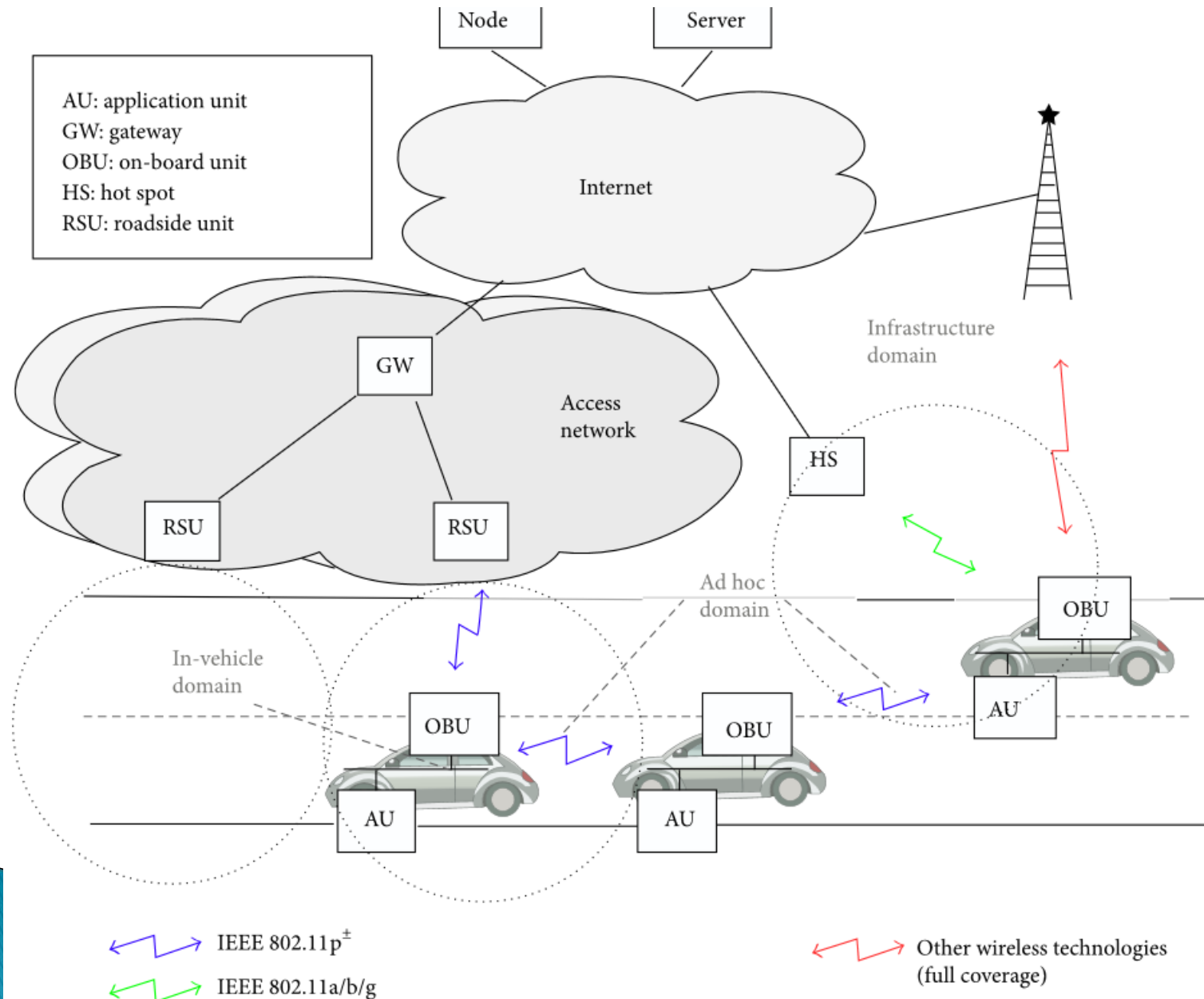
VANET Characteristics

- ▶ The main characteristics of VANETs
 - ❑ High mobility of nodes
 - ❑ Rapidly changing network topology (predictable to some extent)
 - ❑ Unbounded network size
 - ❑ Potential support from infrastructure
 - ❑ Real time , time-sensitive data exchange
 - ❑ Crucial effect of security and privacy
- 

CAR-2-CAR communication consortium reference architecture (C2C CC)

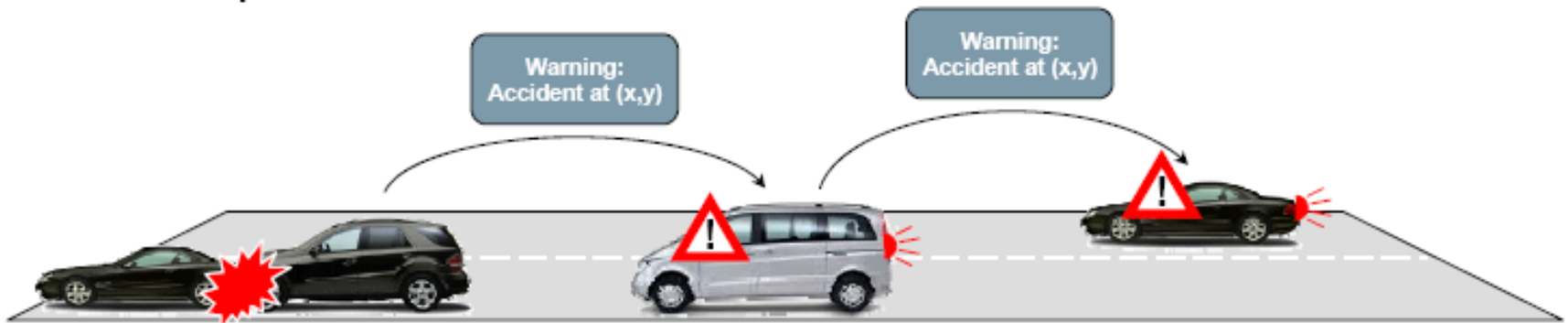
- ▶ The in-vehicle domain is composed of an on-board unit (OBU) and one or multiple application units (AUs).
- ▶ The connections between them are usually wired and sometimes wireless.
- ▶ However, the ad hoc domain is composed of vehicles equipped with OBUs and roadside units (RSUs).
- ▶ An OBU can be seen as a mobile node of an ad hoc network and RSU is a static node likewise.
- ▶ An RSU can be connected to the Internet via the gateway; RSUs can communicate with each other directly or via multihop as well.
- ▶ There are two types of infrastructure domain access, RSUs and hot spots (HSs). OBUs may communicate with Internet via RSUs or HSs.
- ▶ In the absence of RSUs and HSs, OBUs can also communicate with each other by using cellular radio networks (GSM, GPRS, UMTS, WiMAX, and 4G)

C2C-CC reference architecture

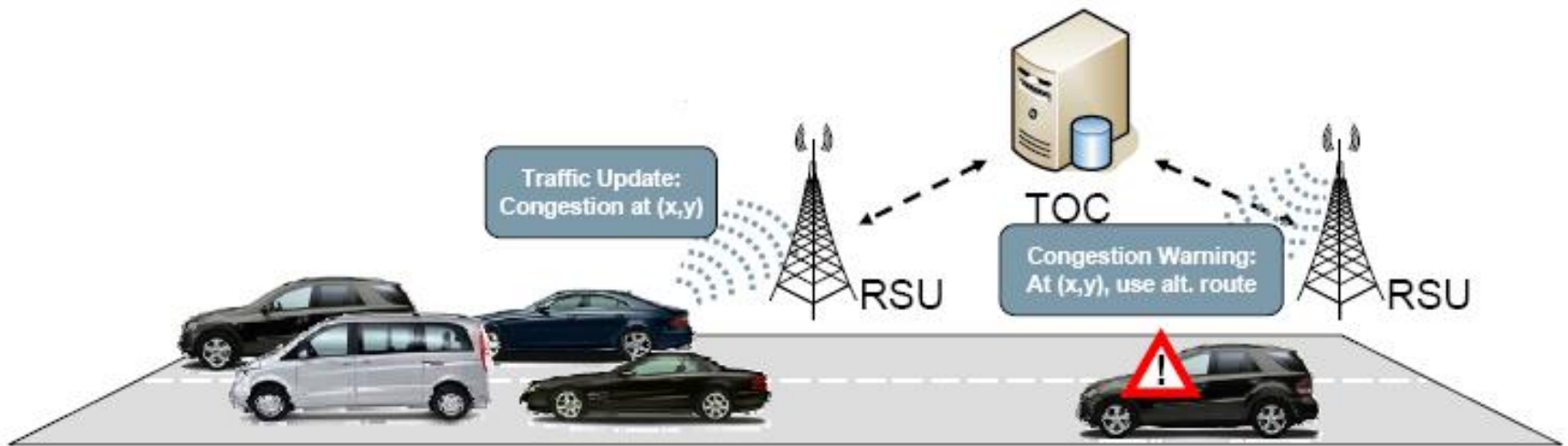


Objectives

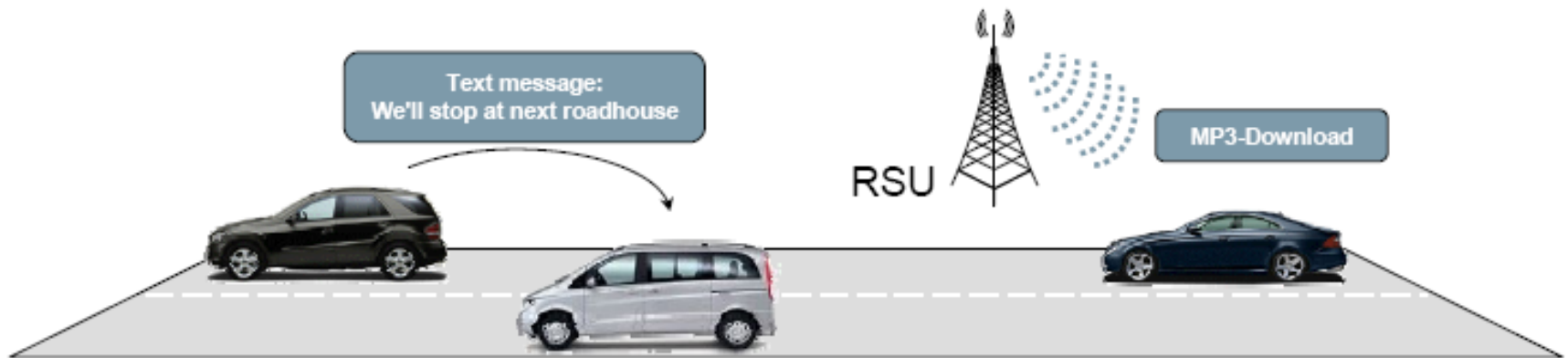
- ▶ VANETs promises safer roads, assures less or no accidents.



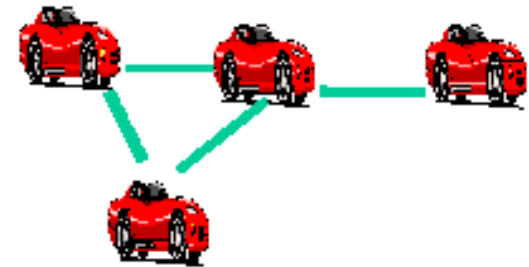
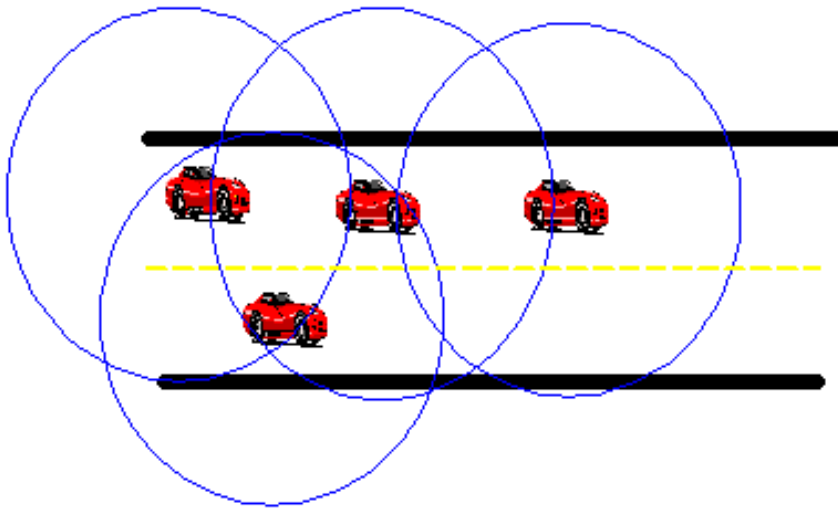
- ▶ More efficient driving
- ▶ By letting the driver know about the traffic.



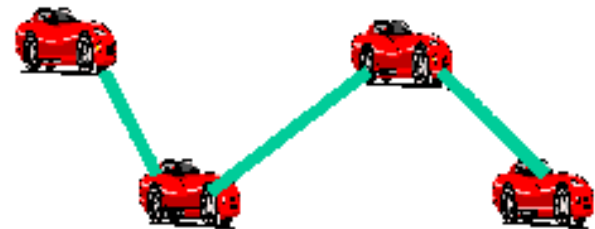
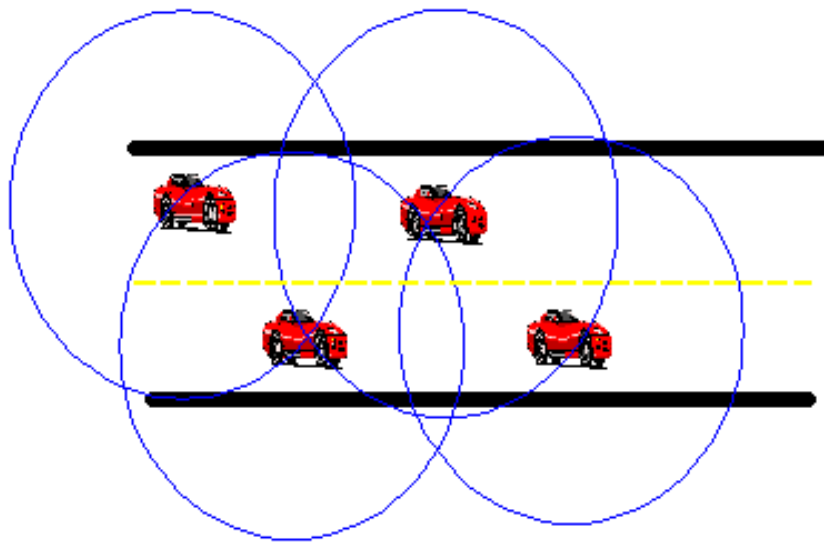
► More fun and entertainment



- ▶ Message propagates to destination using a number of intermediate links

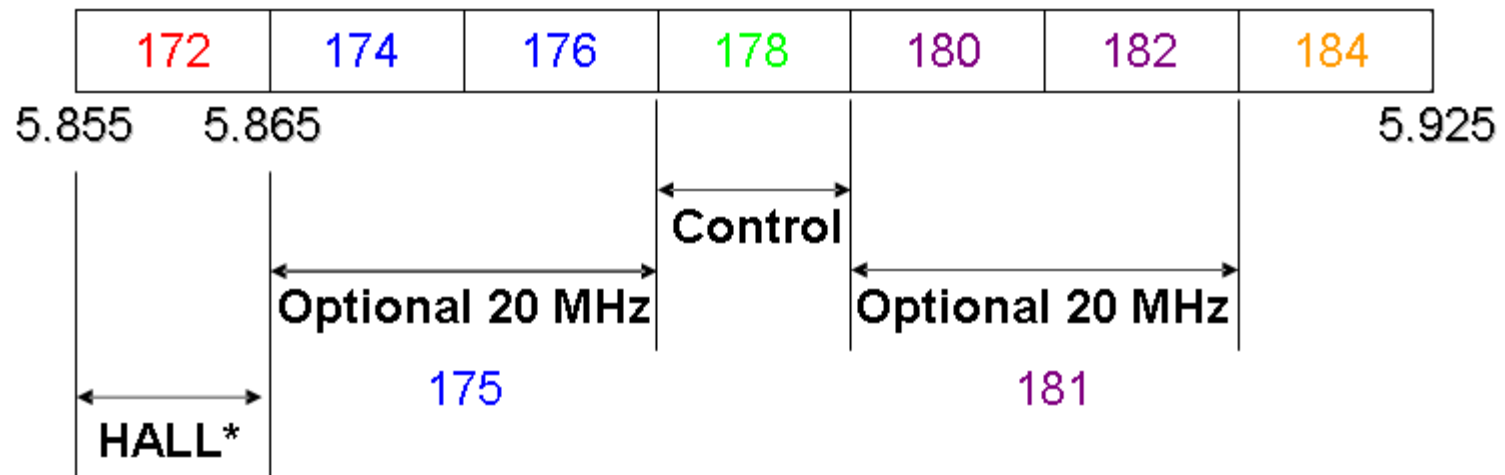


- ▶ If vehicle mobility causes links to break, message rerouted using a different path



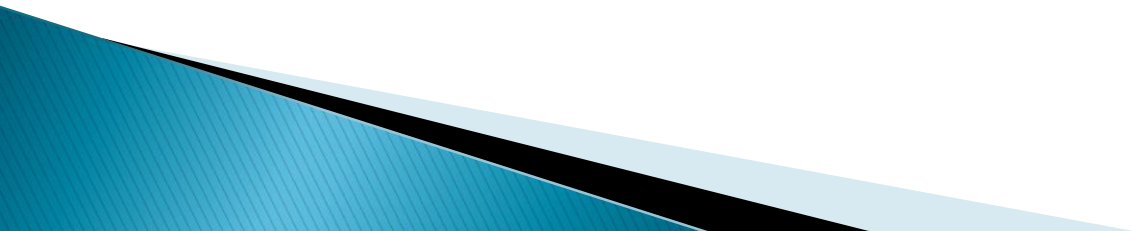
Dedicated Short Range Communications (DSRC)

- ▶ DSRC operates at 5.9 GHz



***High Availability and Low Latency**

DSRC – Operating Characteristics

- ▶ IEEE 802.11p protocol (802.11a modification for VC)
 - ▶ Maximum range: 1000 m
 - ▶ Vehicle speeds up to 100 mph
 - ▶ Low latency: 50 ms
 - ▶ Application priority: 8 levels
 - ▶ Channel 172: vehicle safety only
- 

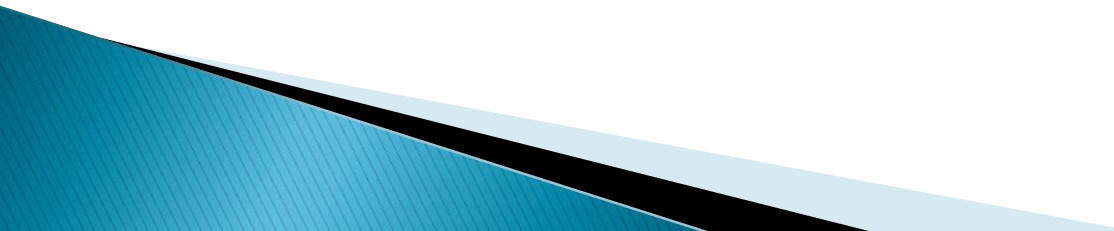
How does DSRC work?

- ▶ Road-Side Unit (RSU)
 - Announces to OBUs 10 times per second applications it supports on which channel
- ▶ On-Board Unit (OBU)
 - Listens on Channel 172
 - Executes safety applications first
 - Then switches channels
 - Executes non-safety applications
 - Returns to Channel 172 and listens

Differences from manet

- ▶ Limited Redundancy
 - The redundancy in MANETs is critical to providing additional bandwidth
 - In VANETs the redundancy is limited both in time and in function
- ▶ Rapid Topology Changes
 - High relative speed of vehicles => short link life
- ▶ large scale – potentially billion

VANET applications

- Safety alerts
 - Requirement: Bounded latency
 - Primary Issue: Broadcast storm
 - Congestion warning
 - Requirement: Message persistence
 - Primary Issue: Disconnected network
 - Infotainment
 - Requirement: End-to-end connectivity
 - Primary Issue: Disconnection due to high mobility
- 

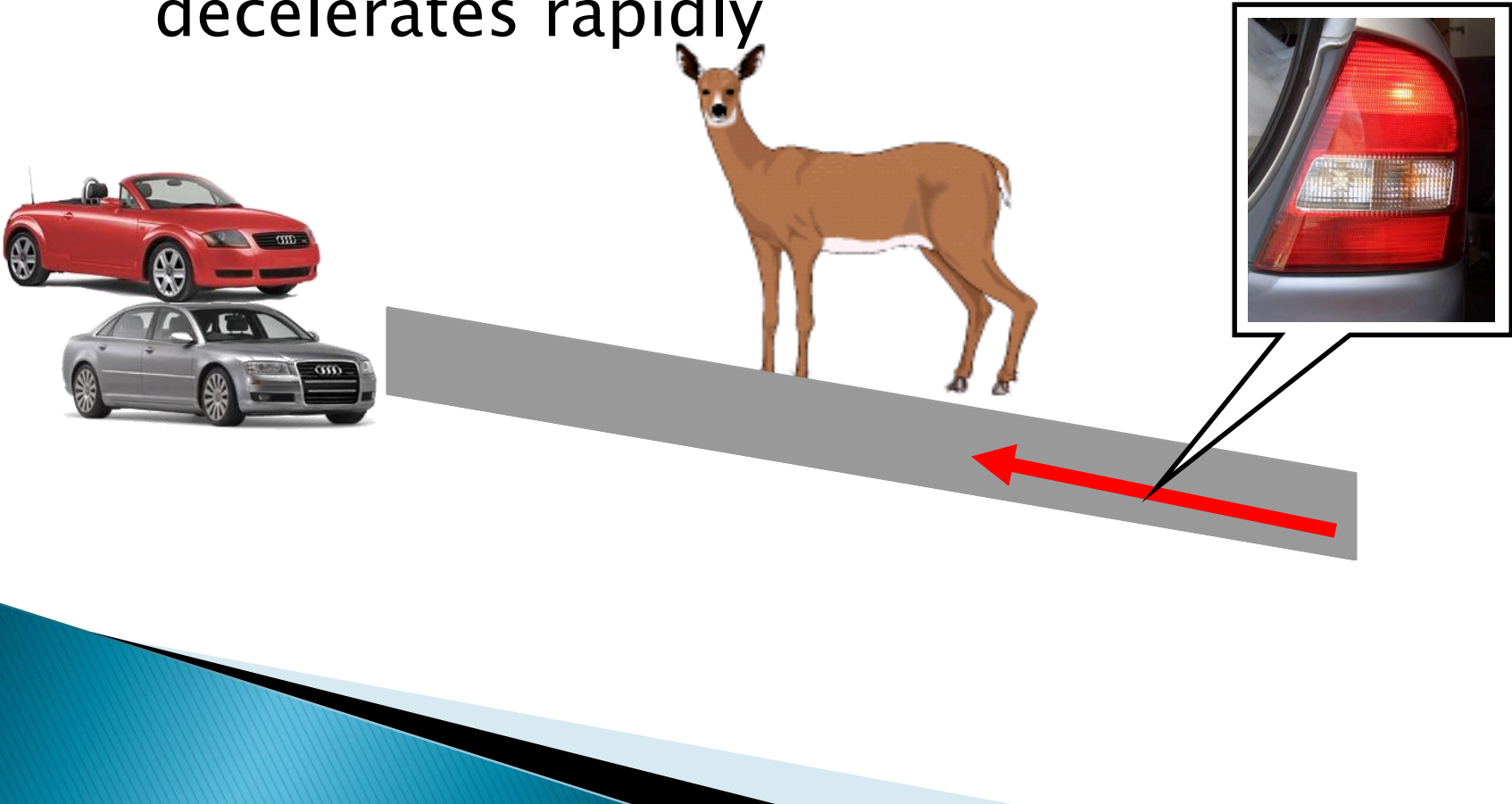
Application-1 :

Congestion Detection

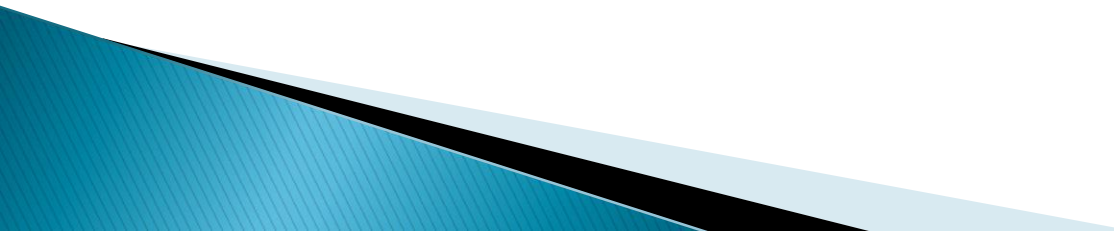
- ▶ Vehicles detect congestion when:
 - # Vehicles $>$ Threshold 1
 - Speed $<$ Threshold 2
- ▶ Relay congestion information
 - Hop-by-hop message forwarding
 - Other vehicles can choose alternate routes

Application-2 : Deceleration Warning

- Prevent pile-ups when a vehicle decelerates rapidly



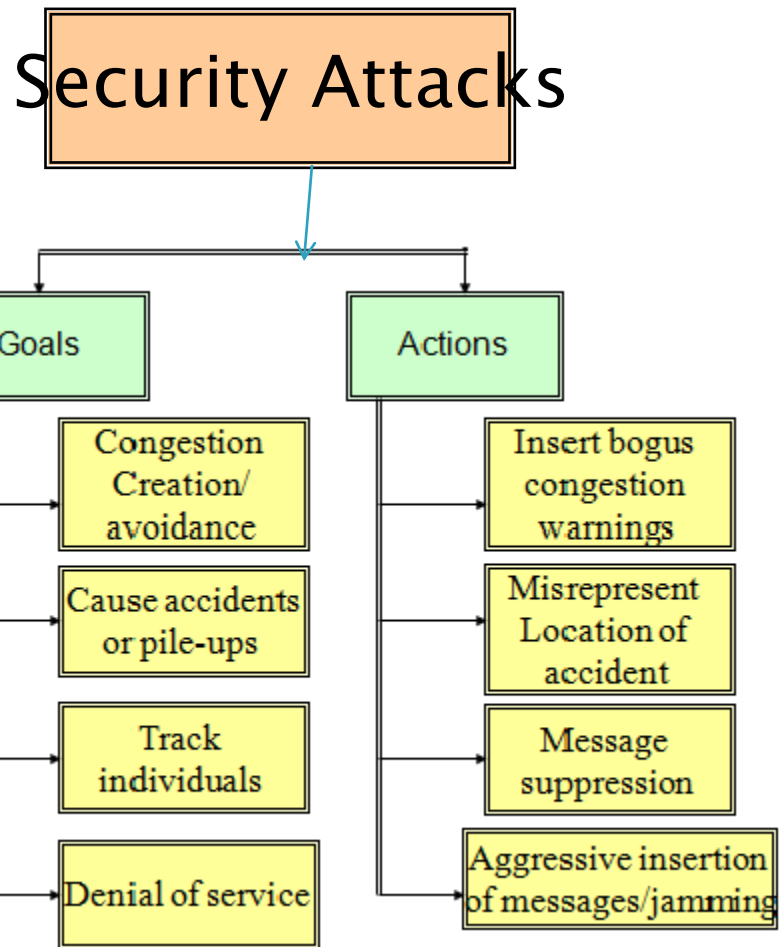
ADVERSARIES

- ▶ A realistic assessment of the vehicular environment suggests the following classes of adversaries
 - ▶ Greedy drivers
 - ▶ Snoops.
 - ▶ Pranksters.
 - ▶ Malicious Attackers.
- 

Attackers

- ▶ Insider or outsider
 - Insider – valid user
 - Outsider – Intruder, limited attack options
- ▶ Malicious or rational
 - Malicious – No personal benefit, intends to harm other users
 - Rational – seeks personal benefits, more predictable attack
- ▶ Active or passive
 - Active: Generates packets, participates in the network
 - Passive: Eavesdrop, track users

attacks



Attacks

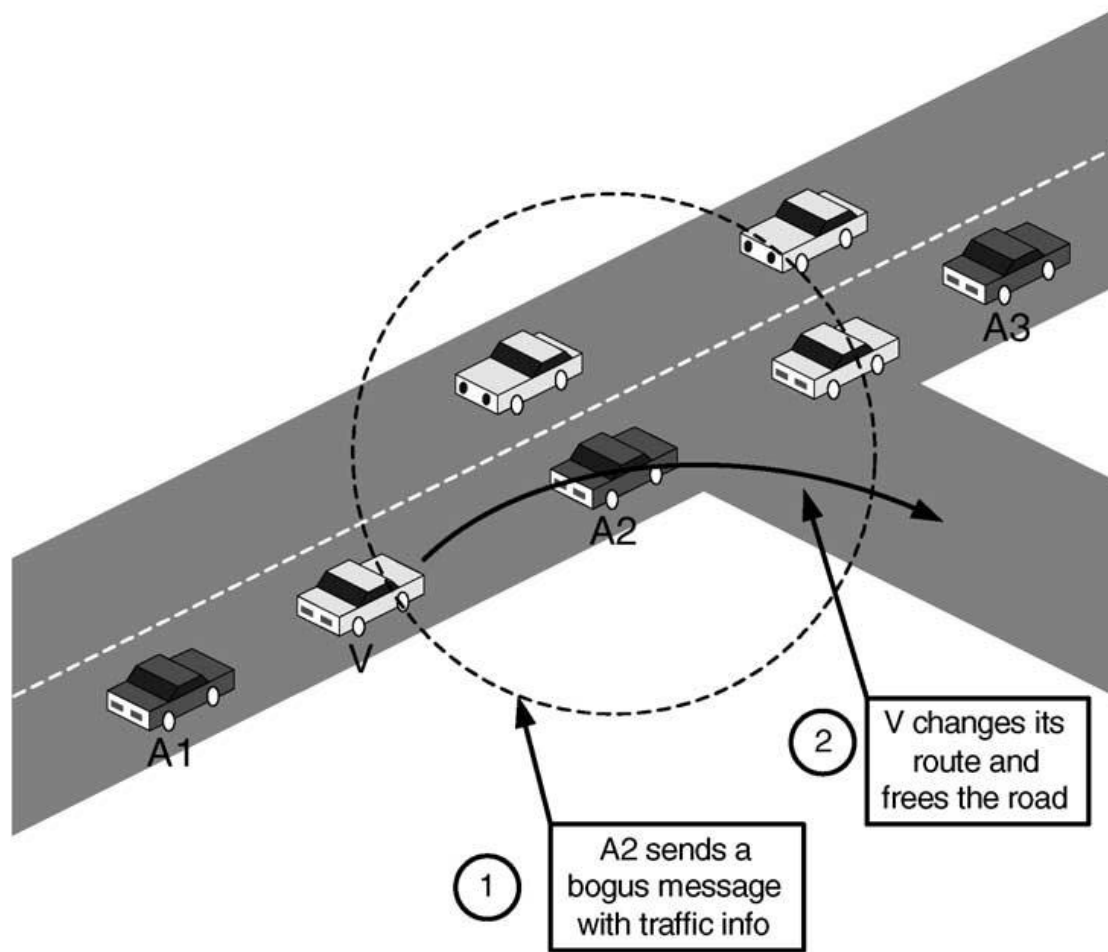
▶ Basic attacks

- Bogus information
- Cheating with sensor information
- ID disclosure
- Denial of service

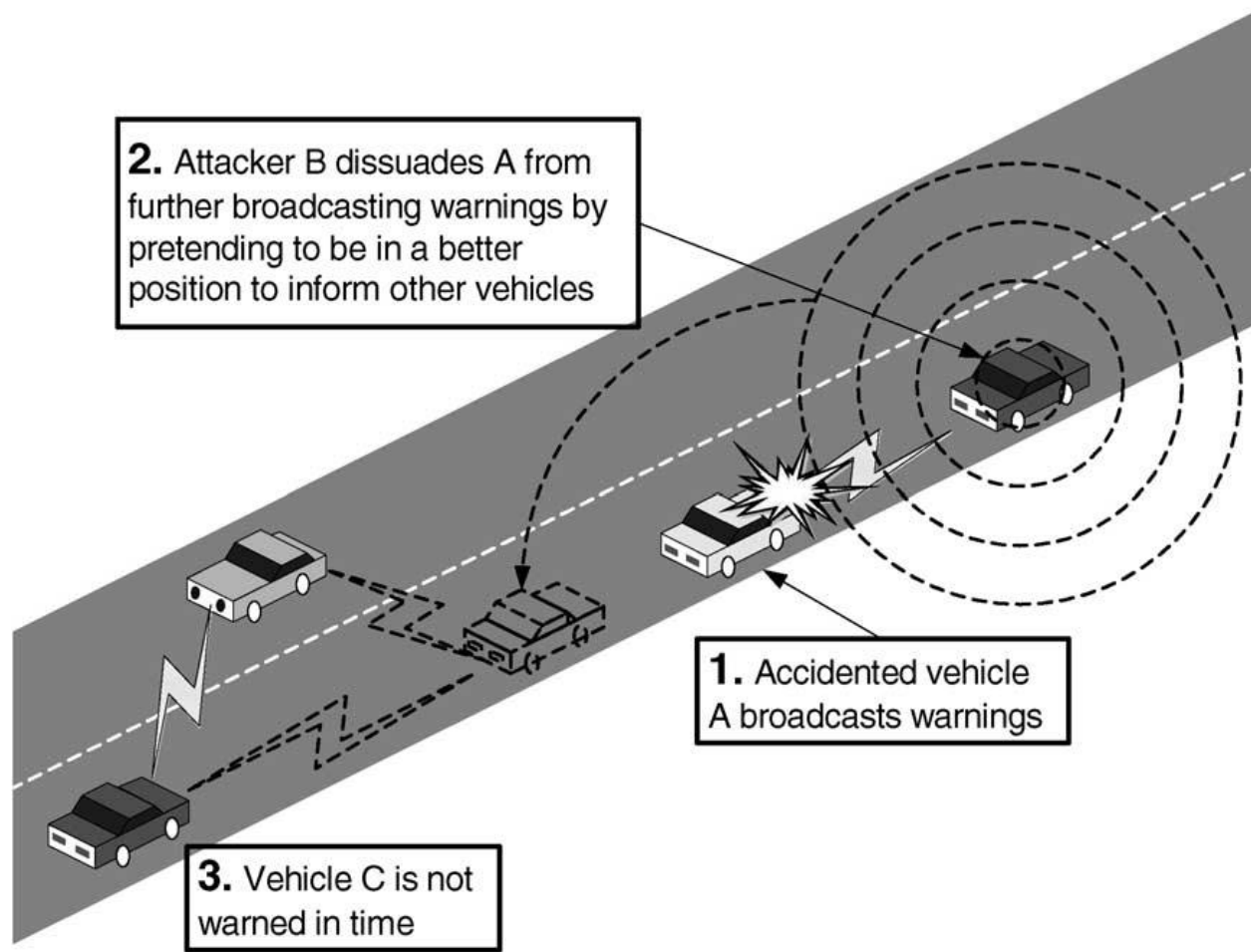
▶ Sophisticated attacks

- Hidden vehicle
- Tunnel attack

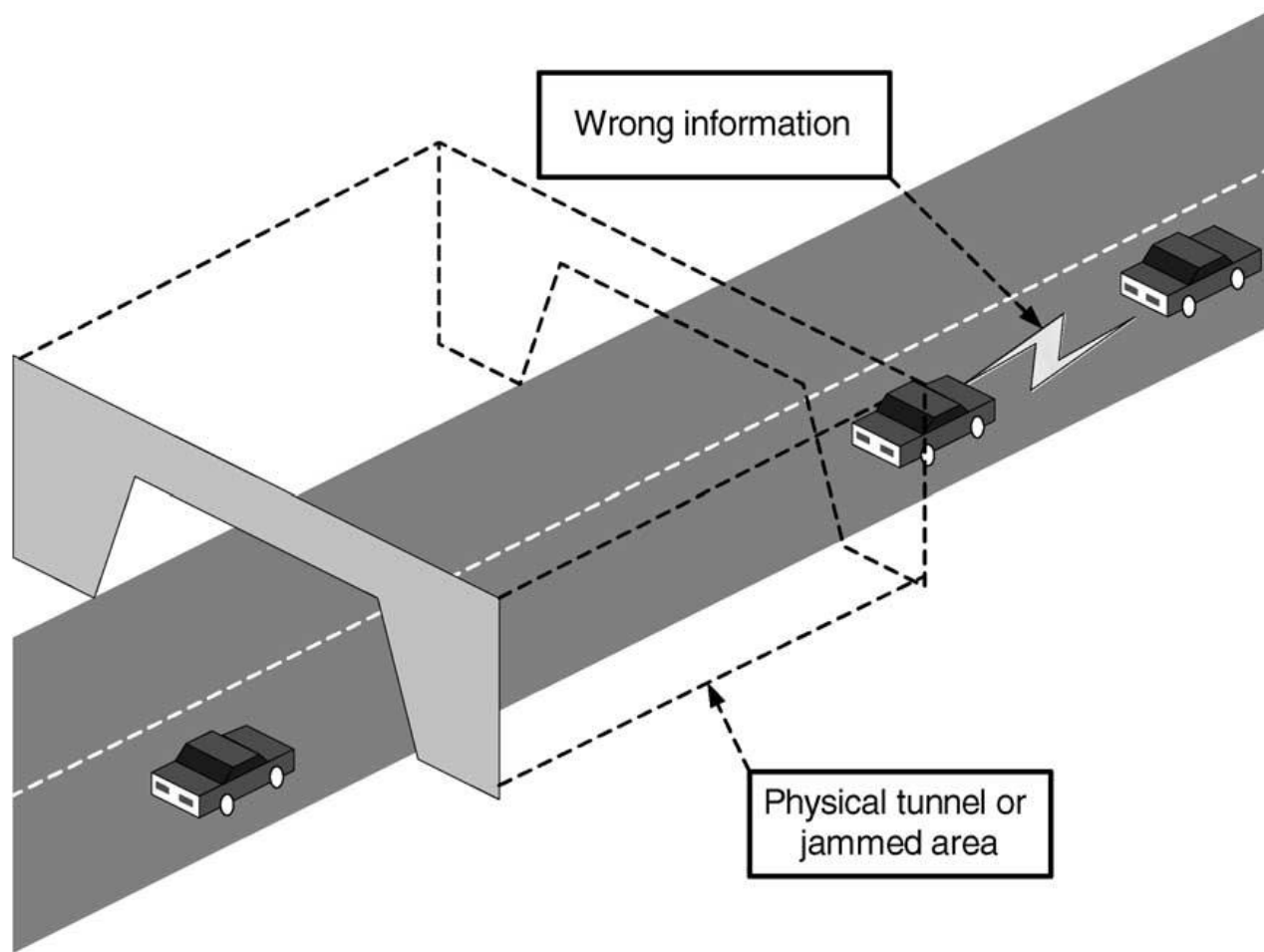
Bogus information attack



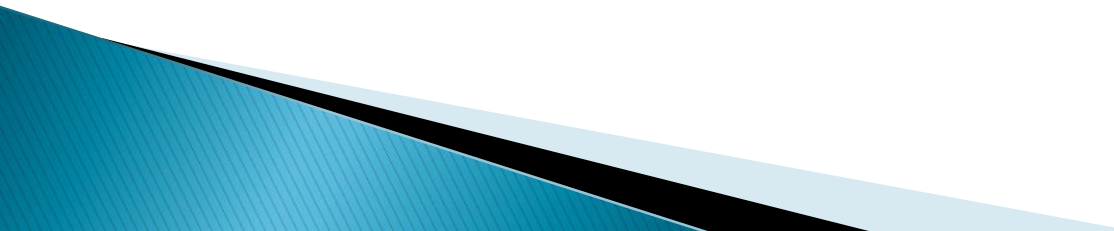
Hidden vehicle attack



Tunnel attack



conclusion

- ▶ In VANETs, vehicles are mobile nodes which communicate with each other and also with Road side unit(RSU).
 - ▶ Provides many useful applications such as traffic optimization, payment services, location-based services, infotainment.
 - ▶ We have analyzed the threat, general classification of attacks, posed on the vehicular networks.
- 

Reference

- ▶ <http://www.hindawi.com/journals/ijdsn/2015/745303/>

Review Article

Vehicular Ad Hoc Networks: Architectures, Research Issues, Methodologies, Challenges, and Trends

Wenshuang Liang, Zhuorong Li, Hongyang Zhang, Shenling Wang, and Rongfang Bie

College of Information Science and Technology, Beijing Normal University, Beijing 100875, China

Correspondence should be addressed to Rongfang Bie; rfbie@bnu.edu.cn

Received 1 September 2014; Accepted 6 November 2014

Academic Editor: Xiuzhen Cheng

Copyright © 2015 Wenshuang Liang et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Vehicular ad hoc networks (VANETs) have been quite a hot research area in the last few years. Due to their unique characteristics such as high dynamic topology and predictable mobility, VANETs attract so much attention of both academia and industry. In this paper, we provide an overview of the main aspects of VANETs from a research perspective. This paper starts with the basic architecture of networks, then discusses three popular research issues and general research methods, and ends up with the analysis on challenges and future trends of VANETs.

1. Introduction

Recently, with the development of vehicle industry and wireless communication technology, vehicular ad hoc networks are becoming one of the most promising research fields.

VANETs which use vehicles as mobile nodes are a subclass of mobile ad hoc networks (MANETs) to provide communications among nearby vehicles and between vehicles and nearby roadside equipment [1] but apparently differ from other networks by their own characteristics. Specifically, the nodes (vehicles) in VANETs are limited to road topology while moving, so if the road information is available, we are able to predict the future position of a vehicle; what is more, vehicles can afford significant computing, communication, and sensing capabilities as well as providing continuous transmission power themselves to support these functions [2].

However, VANETs also come with several challenging characteristics, such as potentially large scale and high mobility. Nodes in the vehicular environment are much more dynamic because most cars usually are at a very high speed and change their position constantly. The high mobility also leads to a dynamic network topology, while the links between nodes connect and disconnect very often. Besides, VANETs have a potentially large scale which can include

many participants and extend over the entire road network [2].

It is precisely because of both of these unique attractive features and challenging characteristics that VANETs could draw the attention from both industry and academia.

Therefore, several articles have tried to summarize the issues about vehicular networks. For example, in [3, 4], the authors discuss the research challenges of routing in VANETs and then summarize and compare the performance of routing protocols; Hartenstein and Laberteaux present an overview on the communication and networking aspects of VANETs and summarize the current state of the art at that time [5]; Raya and Hubaux address the security of VANETs comprehensively and provide a set of security protocols as well [6]; in [7], the authors propose a taxonomy of a large range of mobility models available for vehicular ad hoc networks. These articles all reviewed specific research areas in VANETs. In addition, others papers like [8] provide comprehensive overview of applications, architectures, protocols, and challenges in VANETs and especially introduce VANETs projects and standardization efforts in different regions (i.e., USA, Japan, and Europe); Al-Sultan et al. provide detailed information for readers to understand the main aspects and challenges related to VANETs, including network

architecture, wireless access technologies, characteristics, applications, and simulation tools [9].

Compared with these current articles, this paper adds the introduction of layered architecture for VANETs so that the summary of network architecture is more complete. Also, we organize the overview of the vehicular ad hoc networks in a novel way. That is, we introduce the VANETs from the research perspective in the paper, including some current hot research issues and general methods, which do good to the progress of VANETs. Moreover, we provide a more comprehensive analysis on VANETs research challenges and future trends, beneficial for further systematic research on VANETs. In summary, this paper covers basic architecture, some research issues, general research methods of VANETs, and some key challenges and trends as well as providing an overall reference on VANETs.

The rest of this paper is organized as follows. Section 2 first introduces the vehicular ad hoc networks architecture, including network components, communication types, and layered network architecture. Then in Section 3, we discuss three aspects of VANETs research issues: routing, security and privacy, and applications. Section 4 focuses on VANETs research methodologies and some VANETs models and simulator tools are also given. Section 5 provides an analysis on VANETs research challenges and future directions. Finally, the paper is concluded in Section 6.

2. Architecture

This part describes the system architecture of vehicular ad hoc networks. We first introduce the main components of VANETs architecture from a domain view. Then, we explain their interaction and introduce the communication architecture. Besides, we provide a presentation of the layered architecture for VANETs.

2.1. Main Components. According to the IEEE 1471-2000 [10, 11] and ISO/IEC 42010 [12] architecture standard guidelines, we are able to achieve the VANETs system by entities which can be divided into three domains: the mobile domain, the infrastructure domain, and the generic domain [13].

As is shown in Figure 1, the **mobile domain** consists of two parts: the **vehicle domain** and the **mobile device domain**. The vehicle domain comprises all kinds of vehicles such as **cars and buses**. The mobile device domain comprises all kinds of portable devices like **personal navigation devices and smartphones**.

Within the infrastructure domain, there are two domains: the **roadside infrastructure domain** and the **central infrastructure domain**. The roadside infrastructure domain contains **roadside unit entities** like traffic lights. The central infrastructure domain contains infrastructure management centers such as **traffic management centers** (TMCs) and vehicle management centers [13].

However, the development of VANETs architecture varies from region to region. In the CAR-2-X communication system which is pursued by the CAR-2-CAR communication consortium, the reference architecture is a little different.

CAR-2-CAR communication consortium (C2C-CC) is the major driving force for vehicular communication in Europe and published its “manifesto” in 2007. This system architecture comprises three domains: in-vehicle, ad hoc, and infrastructure domain.

As shown in Figure 2, the in-vehicle domain is composed of an **on-board unit (OBU)** and one or multiple application units (AUs). The connections between them are usually wired and sometimes wireless. However, the ad hoc domain is composed of vehicles equipped with OBUs and roadside units (RSUs). An OBU can be seen as a mobile node of an ad hoc network and RSU is a static node likewise. An RSU can be connected to the Internet via the gateway; RSUs can communicate with each other directly or via multihop as well. There are two types of infrastructure domain access, RSUs and **hot spots (HSs)**. OBUs may communicate with Internet via RSUs or HSs. In the absence of RSUs and HSs, OBUs can also communicate with each other by using cellular radio networks (**GSM, GPRS, UMTS, WiMAX, and 4G**) [2].

2.2. Communication Architecture. Communication types in VANETs can be categorized into four types. The category is closely related to VANETs components as described above. Figure 3 describes the key functions of each communication type [15].

In-vehicle communication, which is more and more necessary and important in VANETs research, refers to the in-vehicle domain. In-vehicle communication system can detect a vehicle’s performance and especially driver’s fatigue and drowsiness, which is critical for driver and public safety.

Vehicle-to-vehicle (V2V) communication can provide a data exchange platform for the drivers to share information and warning messages, so as to expand driver assistance.

Vehicle-to-road infrastructure (V2I) communication is another useful research field in VANETs. V2I communication enables real-time traffic/weather updates for drivers and provides environmental sensing and monitoring.

Vehicle-to-broadband cloud (V2B) communication means that vehicles may communicate via wireless broadband mechanisms such as 3G/4G. As the broadband cloud may include more traffic information and monitoring data as well as infotainment, this type of communication will be useful for active driver assistance and vehicle tracking.

2.3. Layered Architecture for VANETs. The open systems interconnection (OSI) model is well known to most readers, which groups similar communication functions into one of seven logical layers [16]. The session layer and presentation layer are omitted here, and a given layer can be further partitioned into sublayers in this architecture, as illustrated in Table 1 [17].

Generally, the architecture of VANETs may differ from region to region, and thus the protocols and interfaces are also different among them. For instance, Table 2 illustrates the protocol stack for dedicated short-range communication (DSRC) in the US. DSRC is specifically designed for automotive use and a corresponding set of protocols and standards [17]. The US FCC has allocated 75 MHz of spectrum for

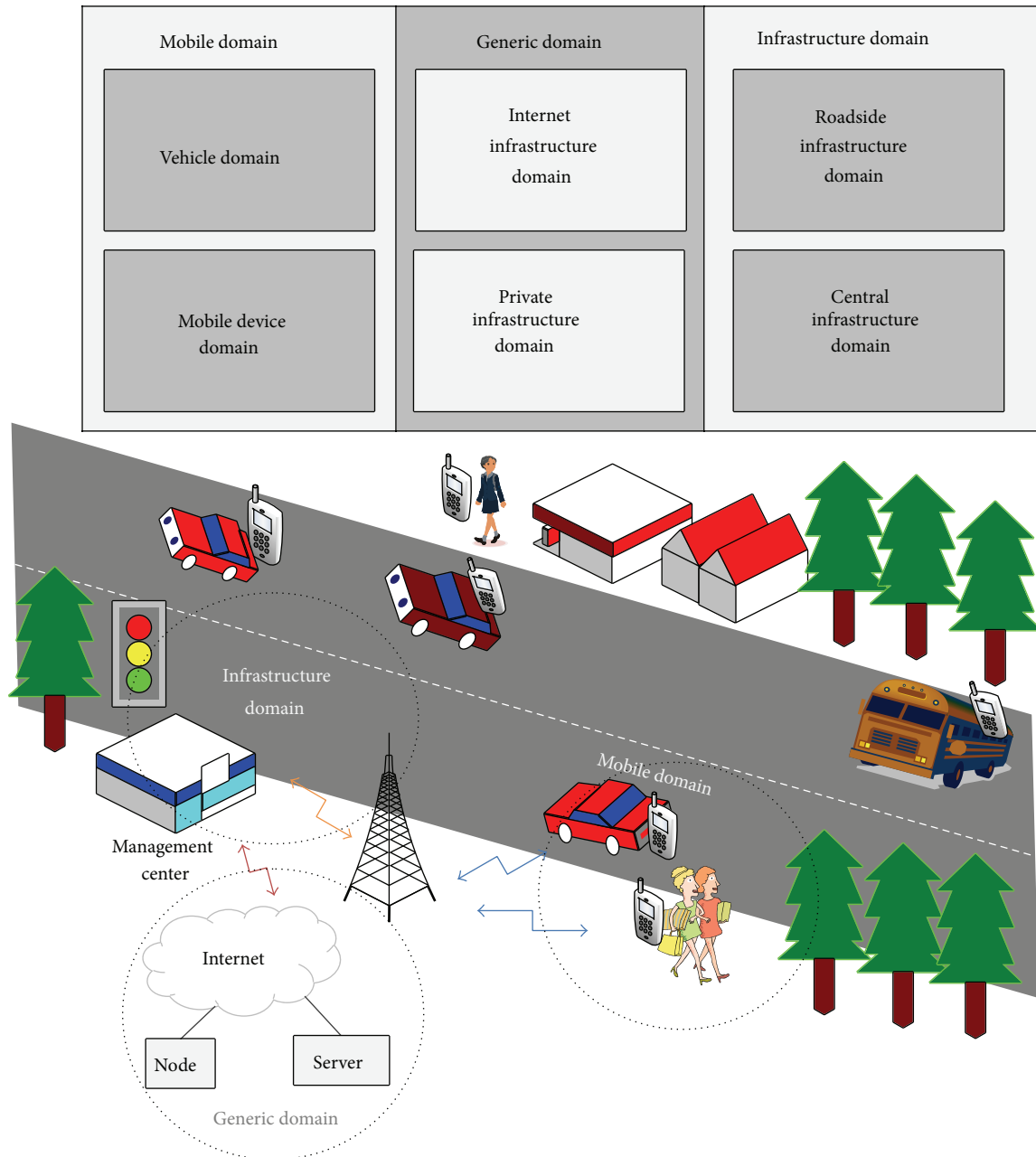


FIGURE 1: VANETs system domains.

DSRC communication, from 5.850 GHz to 5.925 GHz [17]. Different protocols are designed to use at the various layers; some of them are still under active development now. The IEEE 802.11p, an approved amendment to the IEEE 802.11 standard to add wireless access in vehicular environments (WAVE), is focused primarily on the PHY layer and MAC sublayer of the stack. IEEE 1609 is a higher layer standard based on the IEEE 802.11p. IEEE 1609 represents a family of standards that function in the middle layers of the protocol stack to flexibly support safety applications in VANETs, while nonsafety applications are supported through another set of protocols. In particular, network layer services and transport

layer services for nonsafety applications are provided by three quite stable protocols: IPv6, TCP, and UDP [11, 17, 18].

3. Research Issues

This part is a brief introduction to three aspects of VANETs research issues: routing, security, and privacy, as well as applications. Firstly, we discuss the classification of routing protocols and some algorithms. Then state-of-the-art security and privacy researches are discussed. Finally, we introduce two types of applications, namely, safety applications and nonsafety applications.

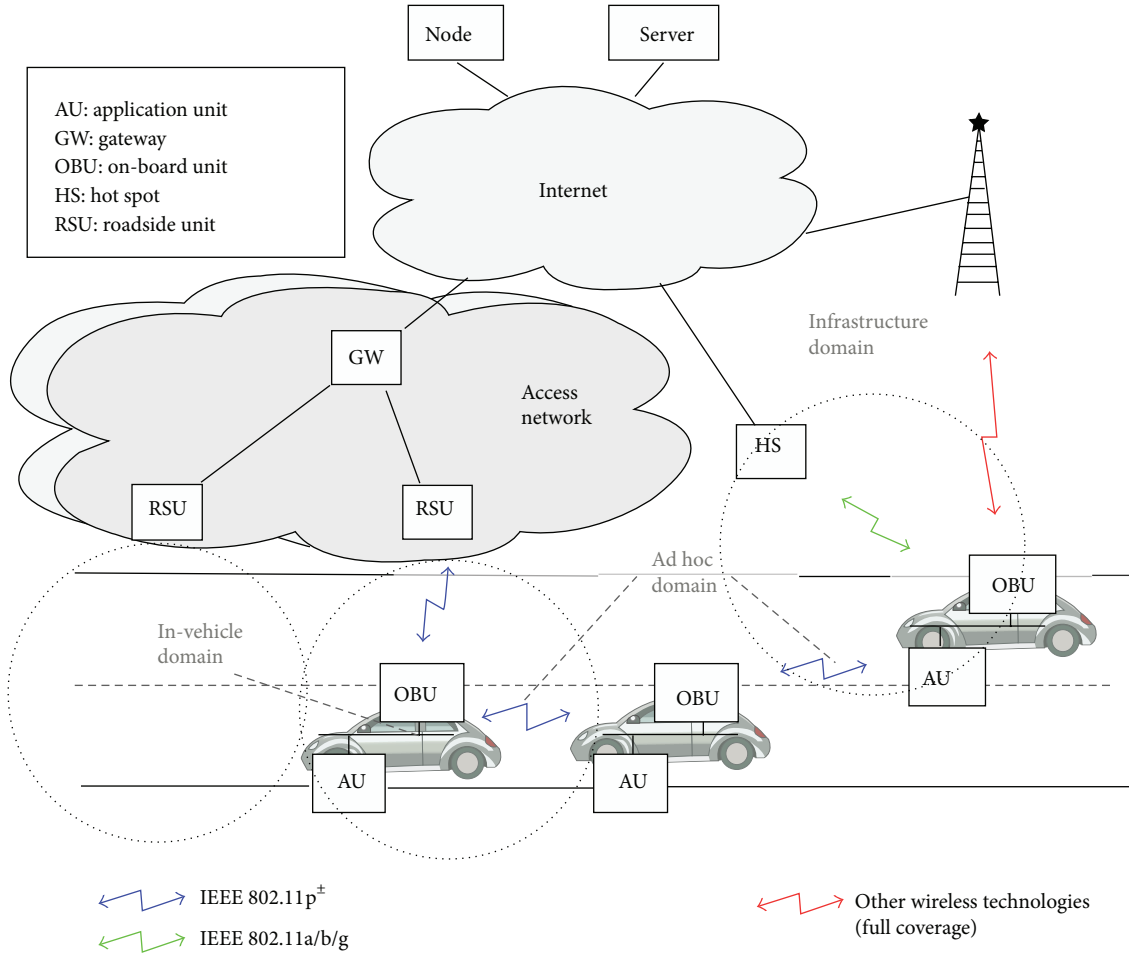


FIGURE 2: C2C-CC reference architecture [14].

TABLE 1: OSI reference architecture.

Application layer	
Transport layer	
Network layer	
Link layer	LLC sublayer
	MAC sublayer
PHY layer	PLCP sublayer
	PMD sublayer

TABLE 2: Layered architecture for DSRC.

Safety applications	Nonsafety Applications
Transport and network layer IEEE 1609.3	Transport layer TCP/UDP
Security IEEE 1609.2	Network layer IPv6
LLC sublayer IEEE 802.2	
MAC sublayer extension IEEE 1609.4	
MAC sublayer PHY layer	IEEE 802.11p

3.1. Routing. In VANETs, wireless communication has been a critical technology to support the achievement of many applications and services. However, due to the characteristics of VANETs such as high dynamic topology and intermittent connectivity, the existing routing algorithms in MANETs are not available for most application scenarios in VANETs. Thus, researchers spare no effort to improve existing algorithms as well as design new ones, so that the communication reliability can be ensured. Depending on the number of senders and receivers involved, routing approaches can be divided into three types: geocast/broadcast, multicast, and unicast approaches.

- (i) *Geocast/Broadcast.* With the requirement of distributing messages to unknown/unspecified destinations, the geocast/broadcast protocols are necessary in VANETs. In [19], the authors review the current message broadcast protocols on vehicular ad hoc networks, such as a spatially aware packet routing algorithm (which predicts the permanent topology holes

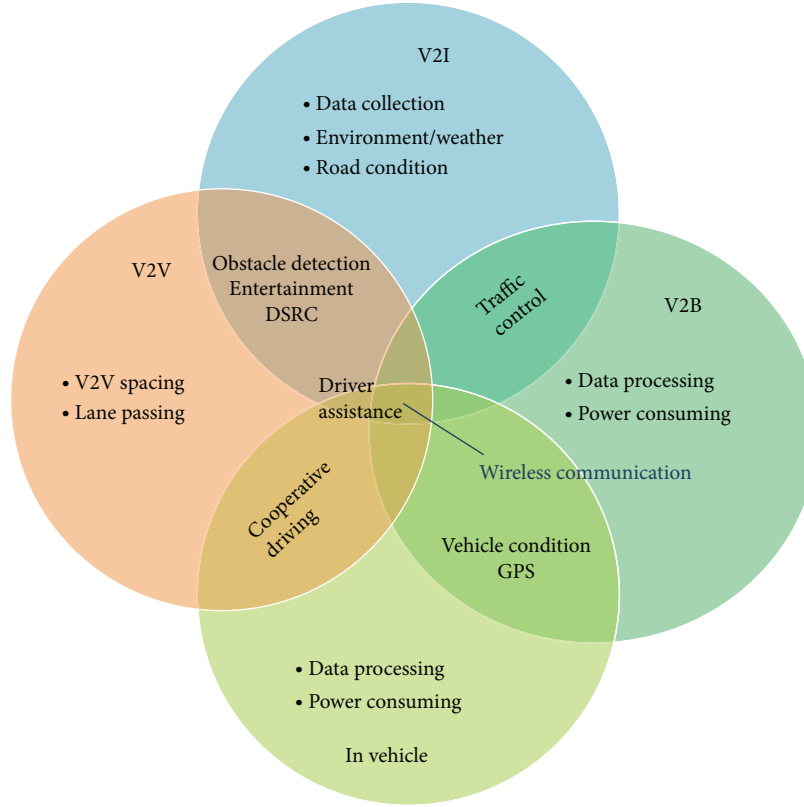


FIGURE 3: Key functions of each communication type.

and conducts the geographic forwarding), SADV (which finds the best path to forward the packet), an interference aware routing scheme (which equips the node with a multichannel radio interface and switches the channels based on the SIR evaluation), FROV (which selects the retransmission spans further node to rebroadcast a message), and a multihop broadcast protocol (which divides the road into segments and chooses the vehicle in the farthest nonempty segment). Other researchers propose some algorithms such as V-TRADE, UMB, AMB, MHVB, and MDDV [20].

- (ii) *Multicast*. Multicast is necessary to communications among a group of vehicles in some vehicular situations, such as intersections, roadblocks, high traffic density, accidents, and dangerous road surface conditions. In [19], the authors categorize the multicast protocols into two main types. One is topology-based approaches, such as ODMRP (which generates a source-based multicast mesh and forwards based on the group address), MAODV (which generates a group-based multicast tree), and GHM (which generates group-based multicast meshes). The other one is location-based approaches, such as PBM (which is based on positions of all one-hop neighbors and positions of all individual destinations), SPBM (which introduces hierarchical group membership management), LBM (which uses a multicast region

as destination information for multicast packets), and RBM and IVG (which define a multicast scope for safety warning messages).

- (iii) *Unicast*. Researchers investigate the unicast communication protocols for VANETs in three ways: (1) greedy: nodes forward the packets to their farthest neighbors towards the destination, like improved greedy traffic-aware routing (GyTAR); (2) opportunistic: nodes employ the carry-toward technique in order to opportunistically deliver the data to the destination, like topology-assist geo-opportunistic routing; and (3) trajectory based: nodes calculate possible paths to the destination and deliver the data through nodes along one or more of those paths, like trajectory-based data forwarding (TBD) [21]. Some of the routing protocols and algorithms are summarized in Table 3.

The above-mentioned protocols are all used to overcome the existing problems of routing in VANETs. Nevertheless, some researchers focus on presenting some novel protocols for V2V and V2I communications of data dissemination. The main contributions are various communication protocols from physical to application layers, even cross-layers. Kim et al. survey ten papers about data dissemination including clusters and channel schemes, mechanisms, protocols, and security in vehicular environments [22]. The results are depicted in Table 4.

TABLE 3: Unicast protocols and algorithms in VANETs.

	Protocols/algorithms	Main ideas
Greedy	Geographical source routing (GSR)	Determines the destination location by RLS (reactive location service)
	Greedy perimeter geographic routing (GPCR)	The packet is greedily forwarded to the junction node (coordinator)
	Improved greedy traffic-aware routing (GyTAR)	Selects junctions based on vehicles traffic density and distance to the destination
	Connectivity-aware routing (CAR)	(1) Greedy forwarding between anchor points along the selected path (2) The packet is forwarded to a node closer to an anchor point
Opportunistic	OPERA: opportunistic packet relaying in disconnected vehicular ad hoc networks	(1) Vehicles moving in the same direction are grouped into clusters (2) Opportunistic technique is used to select a better available path
	Topology-assist geo-opportunistic routing	Uses two-hop beacons for the selection of a forwarding node
	MaxProp	(1) Uses packet priorities to maximize delivery (2) Includes three stages: neighbor discovery, data transfer, and storage management
Trajectory	SiFT	A data forwarder selection decision is shifted from the sender to receiver
	Geographical opportunistic routing (GeOpps)	A data forwarder is selected based on the trajectory information of individual vehicles
	Trajectory-based data forwarding (TBD)	Is based on vehicle trajectory information and traffic statistics
	Two-level trajectory-based routing (TTBR)	(1) The communication area is divided into cells of a grid (2) A grid based location system is applied where some peer servers are distributed

TABLE 4: Ten papers in [22] about data dissemination.

Data dissemination	Main ideas
Road vehicle density-based VANET routing protocol	Uses the road density information as a routing metric to deliver message
An efficient data dissemination protocol	Leverages the resources of parked vehicles at roadside to help in forwarding data
Multiobjective routing protocol (MO-RP)	Is based on a multiobjective metric related to LDP, e2e-delay, and CCI
Dubhe: a reliable and low-latency mechanism	(1) A delay model: makes decisions for path selection (2) An improved greedy broadcast algorithm: boosts the reliability of one-hop data dissemination
Broadcasting protocol with prediction and selective forwarding	Predicts future velocity and selects the best candidate to rebroadcast the message
Two proactive caching and forwarding schemes	(1) One for straight highway sections (2) The other for crossroads and junctions
QoS-enabled handover scheme	Utilizes coordinated multiple point transmission (CoMP) in high speed moving vehicular networks
A secrecy-enhanced relaying protocol	Is based on the network topology and velocity of the moving vehicles
Performance analysis for priority-based broadcast	Analyzes two network models: (1) Markov chain model and (2) queuing model
An adaptive clustering scheme for gateway management	(1) Organizes a two-level cluster architecture gateway system (2) Is employed according to the QoS requirements dynamically

3.2. Security and Privacy. Nowadays more and more intelligent on-board applications may store lots of personal information and vehicular trajectory data, which can disclose individuals' activities, habits, and traces. These threats have to be overcome before communication architecture in VANETs is deployed. Otherwise, the reliability, dependability, and individuals' acceptance of the VANETs system are likely to be low, because attackers may manipulate messages or track the trajectory of vehicles [23, 24].

To address the security and privacy issues, many approaches have been proposed in the literatures over the past few years. Most of them pay more attention to two main aspects: communication and architecture of VANETs [25]. Security architecture is an important part of VANETs to satisfy the requirements of users' security and privacy. In [26], the authors describe the security architecture from several different viewpoints, such as the functional layer view, the organizational/component view, the reference model

view, and the information centric view. In [27], the authors present a novel security architecture focusing primarily on securing the operation of the wireless part of the vehicular communication system and on enhancing the privacy of its users. Different from architecture, the vehicular communication system focuses primarily on secure communication schemes and algorithms [24, 28]. Raya and Hubaux present a communication scheme, in which entities would like to establish a share session key if they need to securely communicate for a long time. This scheme pays much attention to safety-related applications, while the nonsafety-related applications are neglected [6, 29]. In [28], the authors present an advanced secure communication scheme based on Raya and Hubaux's scheme, which extends its session key to be used in nonsafety-related applications and considers two session keys: pairwise and group keys. In [30], the authors discuss many security solutions that have been proposed in detail, such as VPKE (vehicular public key infrastructure), CA (certificate authority), and the group signature.

3.3. Application. Applications in vehicular environment usually can increase the road safety, improve traffic efficiency, and provide entertainment to passengers. In most cases, VANETs applications can be roughly organized into two major classes: safety applications and nonsafety applications.

3.3.1. Safety Applications. Traditionally the intention of safety applications is accident prevention, and thus this kind of applications is also the main motivation for developing vehicular ad hoc networks. Such applications like crash avoidance have a great requirement for the communication between vehicles or between vehicles and infrastructure [9]. Vehicles equipped with various sensors collect traffic data and monitor the environment continuously, and then cooperative vehicular safety applications can change real-time traffic information and send/receive warning messages through V2I or V2V communication to improve road safety and avoid accidents.

Several transportation departments in the US have identified eight safety applications in 2006, which are considered to provide the greatest benefits, that is, traffic signal violation, curve speed warning, emergency brake lights, precrash sensing, collision warning, left turn assist, lane change warning, and stop sign assist [17].

3.3.2. Nonsafety Applications. With respect to their specific intended purpose, nonsafety applications can be classified into several subclasses, such as traffic convenience and efficiency applications, infotainment applications, and comfort/entertainment applications.

Since convenience and efficiency applications can be offered on an individual basis, they do not require standardization and cooperation among vehicles. The growth of such applications and services in the market can be seen in the recent years, including some mobile service offerings on smartphones [13]. Convenience and efficiency applications usually provide drivers or passengers with some useful information, such as weather or traffic information and

the location of restaurants or hotels nearby [9]. Entertainment applications may provide services like media downloading and online games.

4. Research Methodologies

In order to evaluate the performance of different architecture approaches, protocols, algorithms, and applications, an effective research methodology is required in VANETs. Such methods enable researchers and developers to check the drawbacks as well as ensure the availability of new proposed approaches to the above-mentioned aspects. Since VANETs have a potentially large scale, the introduction of a new technology into VANETs requires long development and the experimental implement is very expensive. In general, there are two important and necessary steps before the market introduction: (1) analysis and evaluation by simulations and (2) analysis and verification by field operational testing [13]. In this section, we first introduce the different models which are the essential basis for setting up respective methodologies, and then the simulations and field operational testing are discussed in the following contents.

4.1. VANETs Models. VANETs are a large and complex overall system model, which consists of four submodels for the different aspects: driver and vehicle model, traffic flow model, communication model, and application model [13].

- (i) *Driver and Vehicle Model.* This model aims to reflect the behavior of a single vehicle. This behavior needs to consider two main factors: different driving styles and the vehicle characteristics, such as an aggressive or passive driver and a sports car. In [13], the authors discuss the driver and vehicle model introduced by Treiber et al. or Bayliss.
- (ii) *Traffic Flow Model.* This model aims to reflect interactions between vehicles, drivers, and infrastructures and develop an optimal road network. In [31], according to various criteria (level of detail, etc.), the authors discuss three classes of traffic flow models: microscopic, mesoscopic, and macroscopic.
- (iii) *Communication Model.* This model is a pretty important part of research methodologies to address the data exchange among the road users. Thanks to the constraints of many factors (the performance of the different communication layers, communication environment, and the routing strategies), communication model plays an important role in the research. The authors in [17] give a detailed overview in the research field.
- (iv) *Application Model.* This model is very useful for the market introduction because it can address the behavior and quality of cooperative VANETs applications. This kind of model is necessary for two main reasons: (1) different functionality and visualizations for cooperative applications are provided by different vehicle manufacturers and (2) a prioritization of

the information and warnings is needed among the simultaneous existence of several cooperative applications [13].

4.2. Simulation Methods. Simulation is no doubt an essential step before the implement of new technologies in VANETs. The simulation of VANETs requires two different components: a traffic simulator and a network simulator.

- (i) *Traffic Simulators.* In order to analyze vehicular ad hoc network characteristics and protocol performances, traffic simulators are needed to generate position and movement information of a single vehicle in VANETs environment. In [13], the authors list some existing traffic simulators in detail, like SUMO (simulation of urban mobility) and VISSIM (simulation of the position and movement for vehicles as well as city and highway traffic).
- (ii) *Network Simulators.* To model and analyze the functionality of VANETs, a good network simulator should possess some features including a comprehensive mode, efficient routing protocols like AODV (ad hoc on demand distance vector), and communication standards like IEEE 802.11[p] and IEEE 1609 specifications [13]. Martinez et al. do a comparative study of network simulators, such as GloMoSim (global mobile information simulation) and NS-2 (the most popular simulator for IP-based wired and wireless networks) [32].

4.3. Field Operational Testing. Although the simulation method makes great contributions to the investigation of the VANETs, it does not reflect the real vehicular world. In order to overcome these issues, field operational testing (FOT) has attracted the attention of researchers, which aims to test and evaluate these applications at scale and covers a much wider range of real-world scenarios. Such testing can make the VANETs system closer to the market and generate economic value. Due to the high financial costs and the number of partners, FOT still depends on the reliable results of simulations. On the contrary, the data from the FOT can make the network models more reasonable and improve the performance of protocols. Finally, FOT has four important characteristics: (1) real system components, (2) real vehicles and traffic, (3) including all stakeholders, and (4) large and heterogeneous fleet [13].

5. Challenges and Future Trends

Based on the previous discussion of VANETs, we can see that VANETs are a fantastic self-organizing network for the future intelligent transportation system (ITS). Although researchers have achieved much great progress on VANETs study, there are still some challenges that need to be overcome and some issues that need to be further investigated (e.g., communication, security, applications, stimulation, verification, services, etc.) [15, 33].

5.1. Top Challenges. Compared with MANETs, the specific features of VANETs require different communication paradigms, approaches to security and privacy, and wireless communication systems [34]. For example, network connections may not be stable for a long time period. In order to improve the performance of communication, researchers have investigated the efficient use of available infrastructure, such as roadside units and cellular networks. Although some specific challenges of VANETs have been overcome, many key research challenges have only partially been solved [34]. Thus, researchers need to do deeper work to solve these challenges. In the following discussion, we will summarize the key challenges.

- (i) *Fundament Limits and Opportunities.* Surprisingly little is known about the fundamental limitations and opportunities of VANETs communication from a more theoretical perspective [35]. We believe that avoiding accidents and minimizing resource usage are both important theoretical research challenges.
- (ii) *Standards.* The original IEEE 802.11 standard cannot well meet the requirement of robust network connectivity, and the current MAC parameters of the IEEE 802.11p protocol are not efficiently configured for a potential large number of vehicles [15]. Thus, researchers must do more work about standards.
- (iii) *Routing Protocols.* Although researchers have been presenting many effective routing protocols and algorithms such as CMV (cognitive MAC for VANET) and GyTAR (greedy traffic-aware routing), the critical challenge is to design good routing protocols for VANETs communication with high mobility of vehicles and high dynamic topology [33].
- (iv) *Connectivity.* The management and control of network connections among vehicles and between vehicles and network infrastructures is the most important issue of VANETs communication [36]. Primary challenge in designing vehicular communication is to provide good delay performance under the constraints of vehicular speeds, high dynamic topology, and channel bandwidths [37].
- (v) *Cross-Layer.* In order to support real-time and multimedia applications, an available solution is to design cross-layer among original layers [37]. In general, cross-layer protocols that operate in multiple layers are used to provide priorities among different flows and applications. In [34, 38], the authors address the importance of cross-layer design in VANETs after analyzing the performance metrics.
- (vi) *Cooperative Communication.* In [36], the authors consider the VANETs as a type of cloud called mobile computing cloud (MCC), and in [15] the authors present a broadband cloud in vehicular communication. Thus, the cooperation between vehicular clouds and the Internet clouds in the context of vehicular management applications has become a critical challenge to researchers.

- (vii) *Mobility*. Mobility that is the norm for vehicular networks makes the topology change quickly. Besides, the mobility patterns of vehicles on the same road will exhibit strong correlations [38]. In [29], the authors address the idea that mobility plays a key role in vehicular protocol design and modeling.
- (viii) *Security and Privacy*. Reference [39] presents many solutions that come at significant drawbacks and the mainstream solution still relies on “key pair/certificate/signature.” For example, key distribution is a key solution for security protocols, but key distribution poses several challenges, such as different manufacturing companies and violating driver privacy [38]. Besides, tradeoff of the security and privacy is the biggest challenge under the requirement of efficiency.
- (ix) *Validation*. It is necessary not only to assess the performance of VANETs in a real scenario but also to discover previously unknown and critical system properties. Besides, validation has become more and more difficult under the wider range of scenarios, and Altintas et al. present can use field operational tests (FOTs) to solve this problem, but conducting meaning FOTs is a challenge like a large and complex system with technology components [36].

Thus, considering the characteristics of high mobility and high dynamic topology, researchers still need to study further and find solutions to the challenges we discussed above.

5.2. Future Trends. In the future intelligent society, the potential value of VANETs is unpredictable with safety and entertainment applications. New vehicle applications have recently emerged in several areas ranging from navigation safety to location aware content distribution, commerce, and games [36]. Thus, the VANETs are worthy of further exploration and research, and we believe that there must be more applications and research results in the future. For instance, DSRC technology is proposed to provide a communication link between vehicles and roadside beacons [40] so as to support many applications in vehicular environment. Wu et al. discuss the evolution paths of DSRC and propose several possible enhancements in future versions of DSRC: better channel interleaving and channel coding, better MAC congestion control protocols, more flexibility in channelization, and so forth, [41]. The advanced DSRC can offer the necessary guarantee for the deployment of DSRC-based communication in VANETs. We now discuss some possible future trends of VANETs in three aspects including architecture, algorithm, and application, which we called 3A.

Architecture. In the future, a main research issue of vehicular ad hoc networks focuses on designing an integrated system architecture that can make use of multiple different technologies (e.g., IEEE 802.11p DSRC, WAVE, ITS G5, Wi-Fi, or 3G/4G) and heterogeneous vehicular networks [36]. Besides, in order to deploy the FOT mentioned above, researchers need to design a large scale and complex system architecture which should cooperate with different partners

and manufacturers [13]. Thus, developing a reliable and flexible system architecture is one of the main research trends.

Algorithm. Although the existing algorithms have provided some solutions to some data dissemination problems in VANETs, it is still difficult to examine their performance and security because of the unique features of VANETs. For example, due to the nonpersistent network connections, the end-to-end communication path may not exist. In [42], the authors present the idea that the opportunistic routing algorithm can solve this problem with the carry-forwarding pattern. So the advanced algorithms should be designed with the low communication delay, the low communication overhead, and the low time complexity.

Application. Due to the requirement of continuous awareness of the road ahead, safety applications are still the key research trend in the mobile vehicular environment. However, the authors find no applications following the VANETs application guidelines after studying the most popular vehicular applications in the Android marketplace [43]. So researchers should do more work on standards and security of VANETs applications and investigate the question of “how to use model checking to automatically explore whether these applications meet the standards.”

6. Conclusion

In this paper, we first introduce the VANETs architecture, including network components, communication types, and layered network architecture. Then we discuss three aspects of VANETs research issues: routing, security, and privacy, as well as applications. We also focus on VANETs research methodologies and some mobility models and simulator tools are also given. Finally, we provide an analysis on VANETs research challenges and future trends.

This paper introduces the vehicular ad hoc networks from the research perspective, covers basic architecture, critical research issues, and general research methods of VANETs, and provides a comprehensive reference on vehicular ad hoc networks.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

This research is sponsored by the National Natural Science Foundation of China (61171014, 61272475, and 61371185) and the Fundamental Research Funds for the Central Universities (2013NT57, 2012LYB46) and SRF for ROCS, SEM.

References

- [1] M. Sivasakthi and S. Suresh, “Research on vehicular ad hoc networks (VANETs): an overview,” *Journal of Applied Sciences and Engineering Research*, vol. 2, no. 1, pp. 23–27, 2013.

- [2] H. Moustafa and Y. Zhang, *Vehicular Networks: Techniques, Standards, and Applications*, CRC Press, Boca Raton, Fla, USA, 2009.
- [3] F. Li and Y. Wang, "Routing in vehicular ad hoc networks: a survey," *IEEE Vehicular Technology Magazine*, vol. 2, no. 2, pp. 12–22, 2007.
- [4] X. Su, "A comparative survey of routing protocol for vehicular sensor networks," in *Proceedings of the IEEE International Conference on Wireless Communications, Networking and Information Security (WCNIS '10)*, pp. 311–316, Beijing, China, June 2010.
- [5] H. Hartenstein and K. P. Laberteaux, "A tutorial survey on vehicular ad hoc networks," *IEEE Communications Magazine*, vol. 46, no. 6, pp. 164–171, 2008.
- [6] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *Journal of Computer Security*, vol. 15, no. 1, pp. 39–68, 2007.
- [7] J. Harri, F. Filali, and C. Bonnet, "Mobility models for vehicular ad hoc networks: a survey and taxonomy," *IEEE Communications Surveys and Tutorials*, vol. 11, no. 4, pp. 19–41, 2009.
- [8] G. Karagiannis, O. Altintas, E. Ekici et al., "Vehicular networking: a survey and tutorial on requirements, architectures, challenges, standards and solutions," *IEEE Communications Surveys and Tutorials*, vol. 13, no. 4, pp. 584–616, 2011.
- [9] S. Al-Sultan, M. M. Al-Doori, A. H. Al-Bayatti, and H. Zedan, "A comprehensive survey on vehicular Ad Hoc network," *Journal of Network and Computer Applications*, vol. 37, no. 1, pp. 380–392, 2014.
- [10] M. W. Maier, D. Emery, and R. Hilliard, "Software architecture: introducing IEEE standard 1471," *Computer*, vol. 34, no. 4, pp. 107–109, 2001.
- [11] M. W. Maier, D. Emery, and R. Hilliard, "ANSI/IEEE 1471 and systems engineering," *Systems Engineering*, vol. 7, no. 3, pp. 257–270, 2004.
- [12] D. Emery and R. Hilliard, "Every architecture description needs a framework: expressing architecture frameworks using ISO/IEC 42010," in *Proceedings of the Joint Working IEEE/IFIP Conference on Software Architecture & European Conference on Software Architecture (WICSA/ECSA '09)*, pp. 31–40, Cambridge, UK, September 2009.
- [13] T. Kosch, C. Schroth, M. Strassberger, and M. Bechler, *Automotive Internetworking*, Wiley, New York, NY, USA, 2012.
- [14] CAR 2 CAR Communication Consortium Manifesto, 2007, <http://elib.dlr.de/48380/1/C2C-CC-manifesto.v1.1.pdf>.
- [15] M. Faezipour, M. Nourani, A. Saeed, and S. Addepalli, "Progress and challenges in intelligent vehicle area networks," *Communications of the ACM*, vol. 55, no. 2, pp. 90–100, 2012.
- [16] http://en.wikipedia.org/wiki/OSI_model.
- [17] H. Hartenstein and K. Laberteaux, *VANET-Vehicular Applications and Inter-Networking Technologies*, John Wiley & Sons, 2010.
- [18] http://en.wikipedia.org/wiki/IEEE_802.11p.
- [19] J. Yang and Z. Fei, "Broadcasting with prediction and selective forwarding in vehicular networks," *International Journal of Distributed Sensor Networks*, vol. 2013, Article ID 309041, 9 pages, 2013.
- [20] W. Chen, R. K. Guha, J. K. Taek, J. Lee, and I. Y. Hsu, "A survey and challenges in routing and data dissemination in vehicular ad-hoc networks," in *Proceedings of the IEEE International Conference on Vehicular Electronics and Safety (ICVES '08)*, pp. 328–333, Columbus, Ohio, USA, September 2008.
- [21] A. Wahid, H. Yoo, and D. Kim, "Unicast geographic routing protocols for inter-vehicle communications: a survey," in *Proceedings of the 5th ACM Workshop on Performance Monitoring and Measurement of Heterogeneous Wireless and Wired Networks (PM2HW2N '10)*, pp. 17–24, New York, NY, USA, 2010.
- [22] D. Kim, J. C. Cano, W. Wang, F. de Rango, and K. Hua, "Data disseminations in vehicular environments," *International Journal of Distributed Sensor Networks*, vol. 2013, Article ID 291635, 2 pages, 2013.
- [23] F. Dotzer, "Privacy issues in vehicular ad hoc networks," in *Proceedings of the 5th International Workshop on Privacy Enhancing Technologies (PET '05)*, pp. 197–209, 2005.
- [24] J. M. de Fuentes, A. I. Gonzalez-Tablas, and A. Ribagorda, *Overview of Security Issues in Vehicular Ad-Hoc Networks*, 2010.
- [25] F. Kargl, L. Buttyan, D. Eckhoff, P. Papadimitratos, and E. Schoch, *Working Group on Security and Privacy*, Karlsruhe Institute of Technology, 2011.
- [26] M. Gerlach, A. Festag, T. Leinmüller, G. Goldacker, and C. Harsch, "Security architecture for vehicular communication," in *Proceedings of the 5th International Workshop on Intelligent Transportation (WIT '07)*, 2007.
- [27] P. Papadimitratos, L. Buttyan, T. Holczer et al., "Secure vehicular communication systems: design and architecture," *IEEE Communications Magazine*, vol. 46, no. 11, pp. 100–109, 2008.
- [28] N. W. Wang, Y. M. Huang, and W. M. Chen, "A novel secure communication scheme in vehicular ad hoc networks," *Journal Computer Communications*, vol. 31, no. 12, pp. 2827–2837, 2008.
- [29] M. Raya and J.-P. Hubaux, "The security of vehicular ad hoc networks," in *Proceedings of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN '05)*, pp. 11–21, November 2005.
- [30] G. Samara, W. A. H. Al-Salihy, and R. Sures, "Security issues and challenges of vehicular ad hoc networks (VANET)," in *Proceedings of the 4th International Conference on New Trends in Information Science and Service Science (NISS '10)*, pp. 393–398, Gyeongju-si, Republic of Korea, May 2010.
- [31] S. P. Hoogendoorn and P. H. L. Bovy, "State-of-the-art of vehicular traffic flow modelling," *Proceedings of the Institution of Mechanical Engineers*, vol. 215, no. 4, pp. 283–303, 2001.
- [32] F. J. Martinez, C. K. Toh, J.-C. Cano, C. T. Calafate, and P. Manzoni, "A survey and comparative study of simulators for vehicular ad hoc networks (VANETs)," *Wireless Communications and Mobile Computing*, vol. 11, no. 7, pp. 813–828, 2011.
- [33] S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin, and A. Hassan, "Vehicular ad hoc networks (VANETS): status, results, and challenges," *Telecommunication Systems*, vol. 50, no. 4, pp. 217–241, 2012.
- [34] F. Dressler, F. Kargl, J. Ott, O. K. Tonguz, and L. Wischhof, "Research challenges in intervehicular communication: lessons of the 2010 Dagstuhl seminar," *IEEE Communications Magazine*, vol. 49, no. 5, pp. 158–164, 2011.
- [35] H. Hartenstein, G. Heijenk, M. Mauve, B. Scheuermann, and L. Wolf, *Working Group on Fundamental Limits and Opportunities*, Karlsruhe Institute of Technology, 2010.
- [36] O. Altintas, F. Dressler, H. Hartenstein, and O. K. Tonguz, "Inter-vehicular communication—Quo Vadis," *Karlsruhe Institute of Technology (KIT) Dagstuhl Reports*, vol. 3, no. 9, pp. 190–213, 2014.
- [37] M. Gerla and L. Kleinrock, "Vehicular networks and the future of the mobile internet," *Computer Networks*, vol. 55, no. 2, pp. 457–469, 2011.

- [38] B. Parno and A. Perrig, "Challenges in securing vehicular networks," in *Proceedings of the Workshop on Hot Topics in Networks*, 2009.
- [39] F. Kargl, L. Buttyan, D. Eckho, and E. Schoch, *Working Group on Security and Privacy*, Karlsruhe Institute of Technology, KIT, 2011.
- [40] C. Cseh, *Architecture of the Dedicated Short-Range Communications (DSRC) Protocol*, 1998.
- [41] X. Wu, S. Subramanian, R. Guha et al., "Vehicular communications using DSRC: challenges, enhancements, and evolution," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 399–408, 2013.
- [42] S. Wang, M. Liu, X. Cheng, Z. Li, J. Huang, and B. Chen, "Opportunistic routing in intermittently connected mobile P2P networks," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 369–378, 2013.
- [43] K. Lee, J. Flinn, T. J. Giuli, B. Noble, and C. Peplin, "AMC: Verifying user interface properties for vehicular applications," in *Proceedings of the 11th Annual International Conference on Mobile Systems, Applications, and Services (MobiSys '13)*, pp. 1–12, June 2013.