19

THE NEXT PARADIGM SHIFT: FROM VEHICULAR NETWORKS TO VEHICULAR CLOUDS

Stephan Olariu, Tihomir Hristov, and Gongjun Yan

ABSTRACT

The past decade has witnessed a growing interest in vehicular networking and its vast array of potential applications. Increased wireless accessibility of the Internet from vehicles has triggered the emergence of vehicular safety applications, location-specific applications, and multimedia applications. Recently, Professor Olariu and his coworkers have promoted the vision of Vehicular Clouds (VCs), a non-trivial extension, along several dimensions, of conventional Cloud Computing. In a VC, the under-utilized vehicular resources including computing power, storage and Internet connectivity can be shared between drivers or rented out over the Internet to various customers, very much as conventional cloud resources are.

The goal of this chapter is to introduce and review the challenges and opportunities offered by what promises to be the Next Paradigm Shift:From Vehicular Networks to Vehicular Clouds.

Specifically, the chapter introduces VCs and discusses some of their distinguishing characteristics and a number of fundamental research challenges. To illustrate the huge array of possible applications of the powerful VC concept, a number of possible application scenarios are presented and discussed. As the adoption and success of the vehicular cloud concept is inextricably related to security and privacy issues, a number of security and privacy issues specific to vehicular clouds are discussed as well. Additionally, data aggregation and empirical results are presented.

Mobile Ad Hoc Networking: Cutting Edge Directions, Second Edition. Edited by Stefano Basagni, Marco Conti, Silvia Giordano, and Ivan Stojmenovic.

19.1 BY WAY OF MOTIVATION

The past decade has witnessed a growing interest in vehicular networking and its host of potential applications. The initial vision that had fueled research in vehicular networking had originated in an altruistic impulse, namely that radio-equipped vehicles can somehow network together and, by exchanging and aggregating individual views, can keep the drivers informed about potential traffic safety risks and can heighten their awareness of road conditions and other traffic-related events. The unmistakable promise of vehicular networking has led to a rapid converge with Intelligent Transportation Systems (ITS) leading to the emergence of Intelligent Vehicular Networks, expected to revolutionize the way we drive by creating a safe, secure, and robust environment that will eventually pervade our highways and city streets.

In support of vehicular networking and, more generally, of traffic-related communications, the US Federal Communications Commission (FCC) has allocated 75 MHz of spectrum in the 5.850- to 5.925-GHz band for the exclusive use of Dedicated Short-Range Communications (DSRC) [1]. As pointed out by a number of workers [2–5], the DSRC spectrum by far exceeds the needs of traffic safety applications. The availability of bandwidth has motivated the emergence of a host of third-party applications that can take advantage of the excess DSRC spectrum. Initially, these non-safely-related applications included vehicular *peer-to-peer* (p2p) networking and rudimentary multimedia content delivery. More recently, they were expanded to include location-specific services, and online banking, as well as online gaming and other forms of mobile entertainment. In due time, we expect to see the emergence of a large array of commercial applications targeted at the traveling public and made possible by the excess DSRC bandwidth.

In view of the short communication range stipulated by DSRC, we expect third-party infrastructure providers to deploy various forms of *road-side infrastructure* as well as advanced in-vehicle resources such as embedded powerful computing and storage devices, cognitive radios, and multimodal programmable sensor nodes. As a result, in the near future, vehicles equipped with computing, communication, and sensing capabilities will be organized into ubiquitous and pervasive networks with a significant Internet presence while on the move. This will revolutionize the driving experience making it safer, more enjoyable, and more environmentally friendly [6]. As a pleasant side benefit, the unsightly billboards that flank our highways will disappear and will be replaced by in-vehicle advertising that the driver can filter according to their wants and needs. However, we believe that the impressive array of on-board capabilities present in our vehicles is likely to remain underutilized by the above-mentioned applications.

Under present-day state of the art, the vehicles are mere spectators that witness traffic-related events without being able to participate in the mitigation of their effect. We suggest that in such situations the vehicles have the potential to cooperate with various authorities to solve problems that otherwise either would take an inordinate amount of time to solve (traffic jams) or could not be solved for lack for adequate resources that could be brought to bear. Specifically, we propose to “take vehicular

networks to the clouds" so that the vehicular fleet on our roadways and streets can be integrated with our productivity, comfort, safety, and economic prosperity.

This chapter introduces and promotes our vision of vehicular clouds, a nontrivial extension, along several dimensions, of the conventional cloud computing. Vehicular clouds were motivated by the realization of the fact that, most of the time, the computing and communication resources available in our vehicles are chronically underutilized. Putting these resources to work in a meaningful way will have a significant societal impact. We anticipate that in a vehicular cloud the underutilized vehicular resources including computing power, storage, and Internet connectivity can be shared between drivers or rented out over the Internet to various customers, very much as conventional cloud resources are. We suggest that, even under current technology, many nontrivial forms of vehicular clouds are technologically feasible and economically viable. We fully expect that, once adopted, vehicular clouds will be *the next paradigm shift* with a lasting technological and societal impact.

The idea of a vehicular cloud is novel and so are the potential applications and the significant research challenges that we discuss in the chapter. This is a new concept for which a small-scale prototype is being built by the authors. To the best of our knowledge, no large-scale prototype exists at the moment.

It is appropriate, at this point, to give the reader a synopsis of the chapter. Section 19.2 discusses the vehicular model, the key ingredient in vehicular clouds. Section 19.3 offers an overview of vehicular networks, one of the possible entities that, as we anticipate, will constitute the backbone of vehicular clouds. Section 19.4 provides a succinct overview of cloud computing and cloud services that has motivated the vision of vehicular clouds. Next, in Section 19.5 we introduce vehicular clouds and discuss some of their distinguishing characteristics. The main goal of Sections 19.7 and 19.8 is to illustrate the power of the vehicular cloud concept by enumerating a number of possible application scenarios. Since the adoption and success of the vehicular cloud concept is inextricably related to security and privacy issues, Section 19.9 discusses a number of security and privacy issues specific to vehicular clouds. Further, Section 19.11 discusses in detail a number of fundamental research challenges in vehicular clouds. Section 19.13 discusses issues related to data aggregation in vehicular clouds. Turning to more empirical topics, Section 19.14 reports on our first attempt at studying vehicular clouds empirically by way of simulation in NS-3. Finally, Section 19.16 offers concluding remarks and maps out directions for future investigations.

19.2 THE VEHICULAR MODEL

The past 20 years have seen an unmistakable trend toward making the vehicles on our roads and city streets smarter and the driving experience safer, less stressful, and, as a result, more enjoyable. A typical car or truck today is likely to contain at least some of the following devices: an on-board computer, a GPS device, and a radio transceiver, a short-range rear collision radar device, and a camera, all these supplemented, in high-end models, by a variety of sophisticated sensing devices that can alert the driver to all sorts of mechanical malfunctions and road conditions. In addition, some high-end

vehicles already offer the convenience of an Event Data Recorder (EDR) that collects transactional data from most, if not all, of the vehicle subassemblies. It is, perhaps, not widely known that some GM vehicles as old as model year 1994 were equipped with an EDR-like device able to store retrievable data. In general, the EDRs are intended to be tamper-proof, very much like the well-known black boxes on board commercial and military aircraft.

Somewhat surprisingly, it is also not widely known that in its 2006 ruling [7], the National Highway Traffic Safety Administration (NHTSA) had mandated that EDRs providing tamper-resistant storage of statistical data concerning the car dynamics be installed in most cars starting in September 2010. According to the NHTSA ruling [7], by September 1, 2010 an EDR device must be installed in light vehicles (i.e., those vehicles with unloaded weight of 5500 lb or less). In the light of this, it is reasonable to assume that in the near future, at least in the United States, even low-end vehicles will be fitted with an on-board GPS device and with a tamper-resistant EDR.

The EDR is responsible for recording essential mobility attributes including acceleration, deceleration, lane changes, sensor and radar readings, and other similar data. Each piece of logged data is duly documented and associated with an instantaneous GPS reading. As a consequence, given a time interval of interest, the EDR stores information such as the highest and lowest speed, the position and time of the strongest acceleration/deceleration during that time interval, as well as location, time, and target lanes in the various lane changes made in the time interval of interest. In addition, all of the vehicle's subassemblies, including the speedometer, engine sensors, gas tank sensors, tire pressure sensors, and sensors for outside temperature, feed their own readings into the EDR. These subassemblies report such attributes as the current geographic position, current speed, momentary acceleration or deceleration, lane changes, road surface temperature, and the presence of black ice.

The EDR is also fitted with a cell-phone programmed to call predefined numbers (including, e.g., E-911) in the case of an emergency. Such a system is an important life-saving device since in case of an accident the driver may be incapacitated and may be physically unable to place the call. As already mentioned, this useful feature is already offered in some high-end vehicles and is essential for reporting, upon the deployment of an airbag, that the vehicle was probably involved in a collision.

Among other things, EDR-provided data can be used by fleet operators to optimize the up-time of vehicles by sophisticated self-checks and by scheduling vehicles for maintenance on a per-need basis as opposed to a fixed calendar date.

Being tamper-free, the EDRs are expected to have a huge societal impact promoting, among others, less aggressive driving habits and a better awareness of social responsibility. In turn, as pointed out by Palmer [8], this is expected to reduce the number and severity of traffic accidents.

As technology is moving closer and closer to packing sophisticated resources in individual vehicles, many manufacturers and federal agencies are turning their attention to making the vehicles on our roads more fuel- and energy-efficient than ever. See, for example, references 6 and 9–11, among many other relevant sources.

It is sufficient to recall that the past decade has seen the emergence of hybrid vehicles from the automotive engineers' drawing board into production, to the point

where today half a dozen car and truck manufacturers offer hybrid vehicles on the North American market [12].

In addition to their sophisticated array of sensing and computation capabilities, the availability of virtually unlimited power supply and growing Internet presence will make our vehicles perfect candidates for housing powerful on-board computers augmented with huge storage devices that, collectively, may act as networked computing centers on wheels [13,14].

19.3 VEHICULAR NETWORKS

Wireless technology was available for the past 60 years; yet, with few exceptions, it did not find its way into the arena of vehicular communications until very recently. In order to understand the sea change that we have witnessed in the past decade or so, it helps to recall that the US Department of Transportation (US-DOT) estimates that in a single year, congested highways due to various traffic events cost over $75 billion in lost worker productivity and over 8.4 billion gallons of fuel [9]. The US-DOT also notes that over half of all congestion events are caused by highway incidents rather than by rush-hour traffic in big cities [7]. Further, the NHTSA indicates that congested roads are one of the leading causes of traffic accidents. Extrapolating from January–September 2009 statistics (the latest available official data), the NHTSA predicted for 2009, an estimated 25,576 fatalities directly attributable to traffic-related incidents [15].

Unfortunately, as noted (among others) by ElBatt et al. [16] and Rybicki et al. [17], on most US highways congestion is a daily event and, with rare exceptions, advance notification of imminent or impending congestion is unavailable. It is worth mentioning that, as pointed out (among others) by Fontaine [13], Misener et al. [18], and Sengupta et al. [19], over the years the ITS community has contemplated several solutions for reducing the effects of congestion. One of the proposed solutions involves adding more traffic lanes to our roadways and streets. While at first sight this seems to be a reasonable course of action, a recent study has pointed out that this strategy is futile in the long run because it is likely to lead to even more congestion and to increased levels of pollution. On the other hand, Fontaine [13] has argued convincingly that given sufficient advance notification, drivers could make educated decisions about taking alternate routes; in turn, this would improve traffic safety by reducing the severity of congestion and, at the same time, save time and fuel.

Under present-day technology, traffic monitoring and incident reporting systems employ inductive loop detectors (ILDs), video cameras, acoustic tracking systems, and microwave radar sensors [20]. As noted by Sreedevi and Black [21] and Varaiya et al. [22], by far the most prevalent among these devices are the ILDs embedded in highways every mile (or half-mile) ILDs measure traffic flow by registering a signal each time a vehicle passes over them. As pointed out by several papers including references 13 and 21, each ILD (including hardware and controllers) costs around $8200; in addition, the ILDs are connected by optical fiber that costs $300,000 per mile. Interestingly, official statistics show that over 50% of the installed

ILD base and 30% of the video cameras are defective (see references 13 and 23). Not surprisingly, transportation departments worldwide are looking for less expensive, more reliable, and more effective methods for traffic monitoring and incident detection.

To be effective, innovative traffic-event detection systems must enlist the help of the most recent technological advances. This has motivated extending the idea of mobile ad hoc networks (MANET) to roadway and street communications. The new type of networks, referred to as vehicular ad hoc networks (VANET), that employ a combination of vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications have been proposed to give drivers advance notification of traffic events.

In V2V systems, each vehicle is responsible for inferring the presence of an incident based on reports from other vehicles. Unfortunately, this invites a host of serious and well-documented security attacks intended to cause vehicles to make incorrect inferences, possibly resulting in increased traffic congestion and a higher chance of severe accidents. Not surprisingly, the problem of providing security in VANET has attracted a great deal of well-deserved attention of late as evidenced by a significant number of published works among which we mention references 24–28.

The original impetus for the interest in VANET was provided by the need to inform fellow drivers of actual or imminent road conditions, delays, congestion, hazardous driving conditions, and other similar traffic-related concerns. Therefore, most VANET applications focus on traffic status reports, collision avoidance, emergency alerts, cooperative driving, and other similar concerns [5,29]. Almost across the board, the community of researchers and practitioners anticipate that advances in VANET, or other emerging vehicle-based computing and communications technology, are poised to have a huge societal impact [4,18,30,31]. Because of this envisioned societal impact, numerous vehicle manufacturers, government agencies and standardization bodies around the world have spawned national and international consortia devoted exclusively to VANET. Examples include Networks-on-Wheels, the Car-2-Car Communication Consortium, the Vehicle Safety Communications Consortium, Honda's Advanced Safety Vehicle Program, among many others. We refer the interested readers to the survey articles [4,18] wherein many US and European initiatives and standards are discussed in some detail.

The past few years have witnessed a rapid converge of ITS and VANET leading to the emergence of Intelligent Vehicular Networks with the expectation to revolutionize the way we drive by creating a safe, secure, and robust ubiquitous computing environment that will eventually pervade our highways and city streets.

19.4 CLOUD COMPUTING

Cloud computing (CC) has become synonymous with *hosted services* over the Internet. In reference 32, NIST defined CC as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

As Foley [33] and Hodgson [34] have pointed out, the notion of cloud computing started from the realization of the fact that instead of investing in infrastructure, businesses may find it useful to rent the infrastructure and sometimes the needed software to run their applications. This powerful idea has been suggested, at least in part, by ubiquitous and relatively low-cost high-speed Internet, virtualization, and advances in parallel and distributed computing and distributed databases. One of the key benefits of CC is that it provides scalable access to computing resources and information technology (IT) services. CC is a paradigm shift adopted by a large number of infrastructure providers, both in the United States and around the world, whose large installed infrastructure often goes underutilized. Hand in hand with CC go "cloud IT services" where not only computational resources and storage are rented out, but also specialized services are provided on demand. In this context, a user may purchase the amount of services they need at the moment. As their IT needs grow and as their services and customer base expand, the users will be in the market for more and more cloud services and more diversified computational and storage resources. With CC, developers with innovative ideas for new Internet applications and services are no longer required to have large capital outlays in hardware to deploy their service or more importantly the human expense to operate it. They also need not be concerned with overprovisioning for services whose popularity does not meet their predictions and market analysis, thus wasting costly resources, or underprovisioning for one that becomes wildly popular, thereby missing potential customers and revenue.

From the hardware point of view, three aspects are novel in CC:

- It gives the users the illusion of having infinite computing resources available on demand; thus it eliminates the need for them to plan far ahead for resource provisioning.
- It eliminates the up-front financial commitment by cloud users; thus it allows companies to start small and increase hardware resources only when there is an increase in their needs because of their applications getting more popular.
- It gives the users the ability to pay for computing resources on a short-term basis as needed (e.g., processors by the hour and storage by the day) and release them as needed, thereby rewarding conservation by releasing resources (e.g., machines and storage) when they are no longer useful.

There are, essentially, three distinct instances (types) of CC defined in references 33–37 as:

1. *Infrastructure as a Service (IaaS).* Where the cloud provider offers its customers computing, network and storage resources. Amazon Web Services (AWS) is a very good example of this category where Amazon provides its customers computing resources through its Elastic Compute Cloud (EC2) service and storage service through both Simple Storage Service (S3) and Elastic Book Store (EBS).
2. *Platform as a Service (PaaS).* PaaS solutions are development platforms for which the development tool itself is hosted in the cloud and accessed through

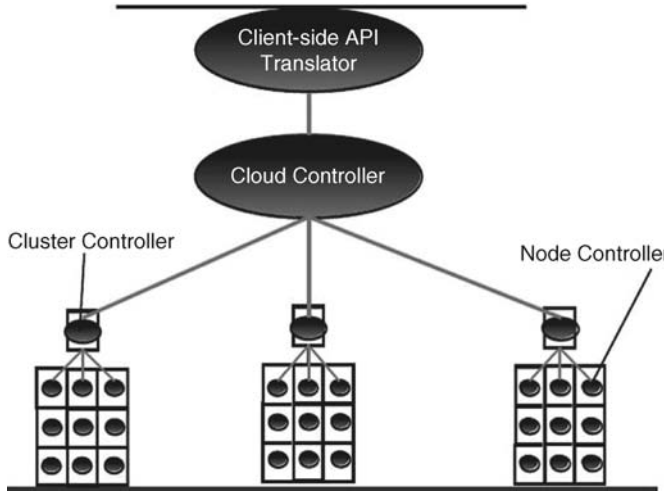

Figure 19.1 The Eucalyptus cloud architecture.

a browser. With PaaS, developers can build web applications without installing any tools on their computers and then deploy those applications without any specialized systems administration skills. Google AppEngine and Microsoft Azure are good examples of this category;

3. *Software as a Service (SaaS).* With SaaS a provider licenses an application to customers as a service on demand, through a subscription, in a "pay-as-you-go" model. This allow customers to use expensive software as much as their application require and no need to pay ahead much money or even hire more operators to install and maintain that software. IBM is a good example of this category.

Figure 19.1 depicts the architecture of the Eucalyptus Enterprise Cloud system [38], which utilizes a typical cloud design. A client application on one side of the network communicates with a cloud controller entity that facilitates the exchange of data to and from multiple services hosted on the back-end. The cloud controller in turn communicates with multiple cluster controllers, which manage multiple node controller entities. In the generic form of the cloud architecture, each of those node controller entities is a software application that runs on top of a server in the datacenter of the company employing the cloud.

19.5 VEHICULAR CLOUDS

As mentioned in Section 19.4, the CC paradigm has worked well for enabling the exploitation of excess computing capacity. We believe it is only a matter of time before the huge vehicular fleets on our roadways, streets, and parking lots will be

recognized as an abundant and underutilized computational resource that can be tapped into for the purpose of providing third-party or community services. It is common knowledge that many of these vehicles spend hours each day in a parking garage, parking lot, or driveway. The computational and storage capabilities of these parked vehicles is a vast untapped resource that, at the moment, is wasted. These attributes make vehicles ideal candidates for nodes in a cloud computing setup, as described above. We conjecture that, given the right incentives, the owner of a vehicle may decide to rent out excess on-board capabilities, just as the owners of large computing or storage facilities find it economically appealing to rent out their excess capacity. For example, as discussed in detail in Section 19.7, we anticipate that while on travel, travelers will "park and plug" their cars in airport parking garages. While in the parking garage, the airport will power the vehicles' computing resources and will allow for on-demand access to this parking garage datacenter. Likewise, the drivers of vehicles stuck in congested traffic will be more than willing to donate their on-board computing resources so that municipal traffic management centers can run complex simulations designed to help alleviate the effects of congestion by citywide rescheduling of traffic lights.

In a series of recent papers [39–43], Professor Olariu and his co-workers have introduced the concept of a *vehicular cloud* (VC) that leverages the excess on-board resources of participating cars. What distinguishes vehicles from nodes in a conventional cloud is the dynamic availability of resources. Clearly, some vehicles are parked for unpredictable periods of time (think of the parking lot of a grocery store) while others are stuck in congested traffic and move at very low speed, changing their points of attachment to some wireless network. Finally, our vehicles spend substantial amounts of time on the road and may be involved in dynamically changing situations; in such situations, the vehicles have the potential to cooperate with local authorities to solve in a timely fashion, traffic-related problems that cannot be addressed by the municipal traffic management centers alone for lack of adequate computational resources. We argue that in many such situations, the vehicles have the potential to cooperatively solve problems that would take a centralized system an inordinate amount of time, rendering the solution useless.

More significantly, we postulate that, in time, the vehicles will autonomously self-organize into clouds utilizing their corporate resources on-demand and largely in real-time in resolving critical problems that may occur unexpectedly. The new vehicular clouds will also contribute to unraveling some technical challenges of the increasingly complex transportation systems with their emergent behavior and uncertainty.

With this in mind, we have coined the term vehicular cloud (VC) to refer to *a group of largely autonomous vehicles whose corporate computing, sensing, communication, and physical resources can be coordinated and dynamically allocated to authorized users.*

In our view, the VC concept is the next natural step in meeting the computational and situational awareness needs not only of the driving public but also of a much larger segment of the population. A primary goal of the VC is to provide on-demand solutions to events that have occurred but cannot be met reasonably with preassigned assets or in a proactive fashion.

It is important to delineate the structural, functional, and behavioral characteristics of VCs. As a step in this direction, in this chapter we identify autonomous cooperation among vehicular resources as a distinguishing characteristic of VCs. Another important characteristic of VCs is the ability to offer a seamless integration and decentralized management of their on-board resources. We anticipate that a VC can dynamically adapt its managed vehicular resources allocated to applications according to changing application-level requirements and environmental and systems conditions.

We believe it is not too far-fetched to imagine, in the not-so-distant-future, a large-scale federation of VCs established ad hoc in support of mitigating a large-scale emergencies. One of these large-scale emergencies could be a planned evacuation in the face of a potentially deadly hurricane or tsunami that is expected to make landfall in a coastal region [14,44–46]. Yet another such emergency would be a natural or man-made disaster apt to destroy the existing infrastructure and to play havoc with cellular communications. In such a scenario, a federation of VCs could provide a short-term replacement for the infrastructure and also provide a decision-support system.

19.6 HOW ARE VEHICULAR CLOUDS DIFFERENT?

While a static VC (e.g., vehicles in a parking lot) may mimic the behavior of a conventional cloud computing facility, most of our vehicles spend a substantial amount of time on the road and may be involved on a daily basis in various dynamically changing situations, ranging from normal traffic to congestion, to accidents, to other similar traffic-related events.

The mobility attribute of the VC, combined with the fact that the presence of vehicles in close proximity to an event is very often an unplanned process, implies that the pooling of the resources of those vehicles that for an VC in support of mitigating the event must occur spontaneously by the common recognition of a need for which there are no preassigned or dedicated resources available. This option does not exist in conventional clouds and turns out to be an important defining characteristic of VCs.

19.6.1 Novel Services Types

There are at least three novel types of cloud computing services made possible by the VC:

1. *Network as a Service (NaaS).* While some vehicles on the road have Internet connection, at the moment it is the case that most cars do not have such a luxury. It is, therefore, natural that the cars with Internet access will offer their excess capacity to the other cars that may need to access the Internet while on the move.

   It is fully expected that many drivers will have persistent connectivity to the Internet through cellular networks and other fixed access points on the road while driving, just imagine how many people have such connectivity through the 3G or 4G cellular network today. This network resource is also expected to

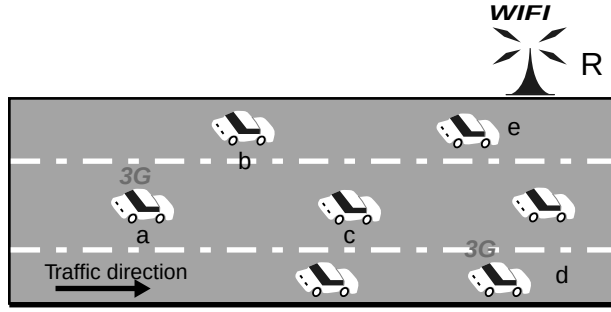

Figure 19.2 Illustrating the NaaS concept.

be underutilized by many drivers because not all of them will be searching or downloading from the Internet while driving, the same as what is happening today on personal computers with cable or DSL connectivity. This important resource can then be shared between drivers on the road, providing Internet to those drivers who are interested to rent it. The expectation is that each driver with Internet connectivity who is willing to share this resource will advertise such information to all vehicles around them on the road. This information may then be multihopped between vehicles, informing them about cars that can act as intermediate hops to the closest access point. Taking the small relative speed between cars on the same direction into consideration, we can look at the system as traditional MANETs, composed of a set of fixed access points and a set of mobile computing nodes moving at a low speed. Thus, any of the existing protocols can be used to allow all vehicles in a given local area to have connectivity to the Internet through available access points or cars with Internet connectivity.

Figure 19.2 shows an example of cars on the road where cars *a* and *d* have persistent 3G or 4G Internet connectivity while car *e* has transient WiFi connectivity through the access point *R*. Cars *a* and *d* will periodically broadcast a packet indicating their intention to share the network with other vehicles on the road. On the other hand, car *e* will broadcast a periodic message about its transient WiFi connection to the roadside *R*. If any car, say *c*, is interested to have Internet access, it may route its requests to any of these cars based on many parameters such as relative speed, expected connection stability, required Internet speed, and expected connection time. For example, if car *c* needs to perform a fast query or to download a small file, it may prefer to route its traffic through car *e* and the access point in turn that has a faster connection speed than the 3G or 4G network. On the other hand, if car *c* needs a stable connection that lasts a longer time, it may route its traffic through car *d* to the 3G or 4G network.

2. *Storage as a Service (STaaS).* While some vehicles have ample on-board storage capabilities, we anticipate that some other vehicles may need extra storage

for their applications. Naturally, the vehicles with excess capacity will be inclined to provide storage as a service. Observe that offering storage as a service in vehicular networks is different from providing computational resources or network access since the potential customers benefit from computing and network access instantly, while they benefit from storage over an extended period of time. It is highly expected that computers on cars will have multiple Terabytes of storage attached to them. This is mainly because of two reasons. First, persistent storage is becoming less expensive over time, since terabytes of storage costs nowadays less than $40, which is negligible compared to the cost of the vehicle itself. Second, cars have plenty of space to accommodate multiple hard drives even with today's technology and sizes. Needless to say, having that huge persistent storage setting idle is a waste of resources. This available storage can then be used in many applications in the cloud. Referring to the datacenter at the mall scenario to be discussed in detail in Subsection 19.7.3 later in this chapter, this available storage can be rented out by the mall management as well for customers over the Internet. Another example is to use that storage in content delivery and p2p applications where a file is decomposed into several blocks distributed across nodes of the network and interested users need to collect different blocks to reconstruct the file.

Providing storage as a service in VANET is different from providing computing power or network access in the sense that customers benefit from computing and network access immediately while they expect to benefit from storage over a longer period of time. This is because, as a rule, storage is used for backup purposes or for p2p applications that will benefit later from them. Therefore, for the mall example, cars will leave the mall before customers can make real benefits from their rented storage. This limitation may be a strong obstacle against renting cars storage for backup. However, p2p applications can still be supported by storing multiple replicas of the same file block in many cars; moreover, smaller block sizes should be used. By doing so, cars can still share and send their blocks within any short period of connectivity that may be available through fixed access points or through other cars willing to share their network.

3. *Cooperation as a Service (CaaS)*. Vehicular networks were set up to offer the traveling public a variety of new services ranging from driver safety, to traffic information and warnings regarding traffic jams and accidents, to providing information about weather or road condition, parking availability, and advertisements. As discussed above, 3G and 4G networks and sophisticated Intelligent Transportation Systems (ITS), including deploying costly roadside base stations, can indeed be used to offer such services, but these come with a cost, both at network and hardware levels. We anticipate a new form of *community service*, called CaaS, that will allow providing drivers with a set of services using very minimal infrastructure (i.e., roadside base stations), if they exist, and by taking advantage of V2V communications if no infrastructure is available. CaaS uses a hybrid publish/subscribe mechanism where the driver (or subscriber) expresses his/her interests regarding a service (or a set of services) and where cars having subscribed to the same service will cooperate to provide the

subscriber with the necessary information regarding the service subscribed to, by publishing this information in the network. CaaS may partition the network into clusters, and it uses content–based routing for intra-cluster communications and uses delay and disruption-tolerant network routing for inter-cluster communications.

19.6.2 Security and Privacy Issues in Vehicular Clouds

Security and privacy are the two major concerns when allowing multiple users to share same set of resources, and our mall data center is no exception from that. Essentially, while sharing compute resources between different users, two constraints have to be met. Firstly, the privacy and security of the vehicle's owner should be preserved. Secondly, security and privacy of the customers who rent these resources must also be preserved. Superficially, the security issues encountered in a VC may look deceivingly similar to the ones experiences in other networks. However, a more careful analysis reveals that many of the classic security challenges are either brought about or exacerbated by the characteristic features of VCs to the point where they can be construed as VC-specific. Let us take note of the following VC-specific security issues:

- authentication of high mobility vehicle and of the identity of the owner;
- establishing trust relationships among multiple network nodes;
- scalability to growing VC system;
- preserving the location and privacy of the vehicle and its owner;
- heterogeneous network nodes (many old/new vehicles may not have advanced devices, e.g. GPS and camera sensors).

A partial answer to some of the security and privacy concerns lays in the use of virtualization techniques. In this context, virtualization refers to a concept in which access to a single underlying hardware is coordinated so that multiple guest operating systems can share that single piece of hardware, with no guest operating system being aware that it is actually sharing anything at all.

Thus, with full virtualization, a single computer on a vehicle can be rented to many customers at the same time in addition to the vehicle's owner and none of them will be even aware about the existence of other users on the system. This will basically preserve both the privacy and security of all users on the system. A number of successful virtualization vendors exist today including, among others, Citrix [47] and VMWare [48]. However, VC security presents a number of important facets that are specific to VCs [49–51]. These will be discussed in detail in Section 19.9.

19.7 FEASIBLE INSTANCES OF VEHICULAR CLOUDS

The main goal of this section is to illustrate the power of the VC concept. Due to page limitations, we restrict ourselves to presenting a few possible scenarios that

are feasible for implementation under present-day technology. In Section 19.16 we outline scenarios for VCs that may become feasible once roadside infrastructure becomes more prevalent.

We begin by discussing several possible instances of VCs that aggregate the computing capabilities of parked vehicles. We then move on to dynamic scenarios and show how VCs can be used to mitigate various traffic-related events.

19.7.1 A Datacenter at the Airport

An unmistakable opportunity for a VC is provided by the long-term parking lot of a major airport where cars are parked for days in a row while their owners are on travel. The airport is offering participating cars an Ethernet connection (e.g., 100-Megabit Ethernet, 1G, or even 10G Ethernet connections) as well as access to a power source (e.g., regular power outlet). We refer to this as a "park-and-plug" scenario. The travelers that allow their vehicle to participate in the airport VC will share their travel plans (e.g., their departing and arriving flights), making it easier for the airport to schedule the existing resources. Observe that by virtue of the park-and-plug scenario combined with a detailed travel plan, the long-term parking lot at the airport offers a relatively stable, long-term availability of resources. In addition, anyone who has experienced parking at a major airport knows that the long-term parking lot always seems to be full and finding a parking spot is often a challenge. This indicates that the amount of resources is likely to be plentiful. For a more detailed assessment of the amount of available resources the interested reader is referred to reference 40.

We expect that in the near future the computational resources of the cars in the long-term parking lot of various airports will be pooled together and the corporate resources rented out to various users just like the excess capability of any cloud. In return for their willingness to let their vehicle participate in the VC, the owners may enjoy free parking along with other pecuniary advantages.

19.7.2 A Data Cloud in a Parking Lot

A scenario similar to the one discussed in Subsection 19.7.1 is presented next. Consider a *small-size* business employing about 500 people and specializing in offering IT support and services. It is not hard to imagine that, even if we allow for car-pooling, there will be up to 350 vehicles parked in its parking lot. Day in and day out, the computational resources in those vehicles are sitting idle for hours on end with little or no useful work performed.

The business may proactively seek the formation of a VC by providing appropriate incentives to its employees who will rent the resources of their vehicles to the company on a per-day, per-week, or per-month basis. The resulting VC will harvest the corporate computational and storage resources of the participating vehicles sitting in the parking lot for the purpose of creating a computer cluster and a huge distributed data storage facility that, with proper security safeguards in place, will turn out to be an important asset that the company cannot afford to waste.

Imagine that the business is renting the computational services of a standard cloud. Instead, it could use the idle or underutilized resources in the cars in its own parking lot, rather than going out to rent those resources at great expense. In the scenario above, the architecture of the VC will be almost identical to the architecture of a conventional cloud, with the additional twist of, perhaps, limiting the interaction to weekdays.

We have focused our discussion on a small-size business. One can easily extrapolate to a medium or large business, or a university with hundreds or even thousands of cars parked in its various parking lots. The resources in those cars are likely to sit idle for many hours each day while their owners are at work or taking classes on campus.

19.7.3 A Datacenter at the Mall

Recent US statistics show that day in and day out, mall customers spend hours shopping with some peaks over the weekends or the holiday season. For example, a recent study performed on teens shopping at malls in 2008 showed that 95% of shoppers spent more than one hour at the mall while 68% of them spent more than two hours [52]. Thus, hundreds of thousands of customers visit various malls every day, parking their cars in the mall garage and spending a couple of hours doing their shopping while leaving their computing resources in their vehicles idle during that time.

This underutilized hardware can be used by the mall management, with the driver's permission and consent, to provide "pay-as-you-go" computing resources for customers over the Internet. For example, each car may be equipped with an Ethernet port in the hood. The mall management, on the other hand, may provide an Ethernet cable on each parking spot. Thus, any customer who is interested to share or rent their vehicle's computing resources should plug that cable into their vehicle's Ethernet port.

Observe that the mall management may provide all sorts of incentives to make it attractive for the shoppers to share the resources in their parked vehicles. These incentives may include discounts at various stores at the mall, free parking, and many other similar perks.

Having multiple vehicles connected through Ethernet to a network is, to some extent, similar to having a traditional datacenter where computers are connected with each other. Thus, the mall management can simply use this data center to rent computing power to cloud customers over the Internet same way how Amazon EC2 works now.

19.7.4 Special Event Management

It has been estimated that in the United States there are, annually, more than 24,000 planned special events (e.g., rock concerts, sporting events, and festivals) with an attendance greater than 10,000 people and that, collectively, these special events cause between 93 and 187 million hours of travel delay and between $1.7 and $3.5 billion in additional travel costs [53,54].

In return for, say, free parking, the owners of the many vehicles in the parking lots adjacent to these venues would be more than willing to allow their vehicles

to participate in a VC set up by either the municipality or the event organizers. The unused computing resources in those vehicles could provide the additional computing power needed to calculate dispersal schedules from the event, or develop alternative traffic flow control strategies in response to incidents or changes in desired departure times from an event.

19.7.5 Dynamically Synchronizing Traffic Lights

Imagine a sporting event attended by thousands of people. At the end of the game when everybody tries to leave as soon as possible, a traffic jam may occur. The situation is compounded by static traffic light synchronization. We contemplate a VC involving the cars in the traffic jam; these cars will put their resources at the disposal of a municipal authority in charge of rescheduling traffic lights in such a way as to dissipate the traffic jam as soon as possible. We anticipate that the drivers will be only too willing to let the municipality use the computing power of their cars for the public good which, in this case, is well-aligned with their own personal interests.

Observe that, in this scenario, the municipal authority has the code (program) and the authority to run it. However, they typically do not have the required computational infrastructure on which to run the rescheduling program. This facility is afforded, dynamically, by the VC involving the cars. This scenario suggests a paradigms shift: The basic idea is that the municipality does not have to purchase expensive computing facilities that are very likely to go unused most of the time. Instead the municipality and its Traffic Management Center can harvest, on a per-need basis, the computational resources of the vehicles that happen to witness (be stuck in) a traffic slowdown.

As mentioned before, the ability of vehicles to pool their resources, in a dynamic way, in support of the common good will have a huge societal impact in alleviating, among other things, recurring congestion events that plague our cities around the morning or afternoon rush hour. Also, and very importantly, while congestion is a daily phenomenon, proactively solving the problem is infeasible because of the dynamic nature of the problem and also because of the huge computational effort that its resolution requires. The problem is best solved if and when it occurs in an on-demand fashion dedicating the right amount of resources rather than conservatively pre-allocating abundant resources based on the worst case, which is becoming increasingly infeasible. The key concept that allows the problem to be solved efficiently and economically is the engagement of the necessary resources from the available vehicles participating in the traffic event and their involvement in finding a solution autonomously without waiting for an authority to react to the complicated situation on the ground.

19.8 MORE APPLICATION SCENARIOS

The main goal of this section is to illustrate the power of the VC concept. We touch upon several important scenarios illustrating various aspects of VCs that are extremely important and that, under present-day technology are unlikely to see a satisfactory

resolution. The outlined scenarios are representative of *community* applications intended to mitigate traffic-related problems in a municipality. However, one can easily contemplate extending these scenarios to other application domains.

19.8.1 Dynamic Traffic Signal Optimization

Most traffic signals in the United States run a set of predefined timing plans that set the signal's cycle length and green phase lengths. In most cases, the optimization of signal systems is currently occurring offline at either the isolated intersection or, at best, the corridor level. Timing plans are typically defined for certain time periods, such as the weekday morning or afternoon peak. One of the major disadvantages of this approach is that it requires that data on traffic turning movements be regularly collected to ensure that the signal timing plans are appropriate for current traffic volume conditions. This volume data is then used to develop optimized traffic signal timing plans offline using commercial software packages such as Synchro[1] [55].

A second major disadvantage is that time-of-day-based signal timing plans do not adapt well to unexpected changed in traffic demand. For example, if an incident on the roadway causes travel patterns to change significantly, these signals often cannot fully accommodate these changes in flow, resulting in longer system delays, traffic buildup, and congestion.

Our vision is that the drivers stuck in congested traffic could donate the on-board computing resources in their vehicles so that the municipality could run parallel versions of the signal re-timing optimization software to help improve traffic flow, not only at the corridor level but, indeed, on a wider scale. This would enable traffic signal systems to be more responsive to actual conditions, rather than being based on historic volume counts.

VCs could also offer the opportunity to optimize signal system performance at a municipal level by making dynamic use of vehicular network probe data to re-time signals in a city or county. Detailed arrival information from the vehicular networks could also be used to improve signal system performance.

19.8.2 Dynamic Assignment of HOV Lanes

The scenario discussed in Subsection 19.7.5 has myriad variations ranging from dynamic scheduling of traffic lanes dedicated exclusively to High Occupancy Vehicles (known in the United States as HOV lanes) to establishing various degrees of contraflow on a per-need basis. As pointed out by the US-DOT in its 2008 report and guidelines, "the primary purpose of an HOV lane is to increase the total number of people moved through a congested corridor by offering two kinds of incentives: a savings in travel time and a reliable and predictable travel time. Because HOV lanes carry vehicles with a higher number of occupants, they may move significantly more people during congested periods, even when the number of vehicles that use the HOV

[1] http://www.trafficware.com

lane is lower than that on the adjoining general-purpose lanes. In general, carpoolers, vanpoolers, and transit users are the primary beneficiaries of HOV lanes" [56].

It is, thus, plainly obvious that the main goal of HOV lanes is to promote traffic fluidity and to prevent traffic slowdowns and congestion. It is well known that in most US municipalities, HOV lanes are assigned statically to alleviate congestion induced by rush-hour traffic. However, as we all know, congestion may occur for various other reasons at times other than the end of the work day. Imagine, for example, a situation where the HOV lanes are not used, yet due to some factors, traffic is building up and a congestion or traffic slow-down is imminent. As before, the municipality becomes aware of the impending congestion event and has the authority to mandate to set up HOV lanes but does not have the computational resources to assess the situation and to establish the time frame for using the HOV lane in support of alleviating the effects of the congestion.

Due to insufficient resources (appropriate signs being one key shortcoming), most cities in the United States and Canada only use HOV lanes at rush hour. We believe that VCs could make recommendations for setting up HOV lanes dynamically in the best interest of promoting traffic fluidity and of minimizing travel times for people using the designated HOV lanes. VCs can enable such a dynamic solution by factoring data from sensors on board the individual vehicles (e.g., occupancy sensors) and local traffic intensity in order to optimally configure the HOV lanes. Such a solution is infeasible under present-day technology.

The same idea applies to the strategy of marking certain streets and thoroughfares as *one-way* in support of improving the fluidity of traffic. Again, currently such an approach is infeasible mostly because of insufficient signaling means. This, however, should not be a problem in VC since the drivers will be alerted in real time to road occlusions and other dynamic changes.

19.8.3 Planned Evacuation Management

Another example of a computationally intensive traffic modeling scenario involves assessing evacuations from a metropolitan area. Transportation agencies often develop simulations in order to determine potential traffic control strategies for possible evacuation events. Evacuation events can generally be subdivided into cases where advance notice of an impending event is provided (e.g., a hurricane evacuation) and those cases where no notice of the event is provided (e.g., a chemical spill, nuclear reactor accident, or terrorist attack).

In cases of predicted disasters, such as hurricanes, massive evacuations are often necessary in order to minimize the impact of the disaster on human lives. However, there are several issues involved in a large-scale evacuation. For example, once an evacuation is under way, finding available resources, such as gasoline, drinking water, medical facilities, and shelter, quickly becomes an issue. In its recent report on hurricane evacuations [14], the US-DOT found that emergency evacuation plans often do not even consider availability of such resources. The US-DOT also determined that emergency managers need a method for communicating with evacuees during the evacuation in order to provide updated information. The report suggested that traffic

monitoring equipment should be deployed to provide real-time traffic information along evacuation routes.

We now point out natural ways in which VC can work with the emergency management center overseeing the evacuation in order to provide travel time estimates, notification of available resources (such as gasoline, food, and shelter), and notification of contraflow roadways to the evacuees. We anticipate that the vehicles involved in the evacuation will self-organize into one or several interoperating vehicular clouds that will work hand in hand with the emergency management center. In the course of this interaction, the emergency managers can upload information about open shelters to the central server.

It is important to note that this system would be used to facilitate an evacuation before disaster strikes, so we assume that electricity and network connections are available. In addition to having state authorities send information to the VCs about evacuations or contraflow lanes, using role-based communication as described earlier, the VCs themselves could determine the direction and speed that traffic is flowing. The evacuees entering entrance ramps onto contraflow roadways (these ramps would likely have been used as exit ramps previously) will be alerted to the direction that traffic is moving. The VCs could also alert drivers to upcoming entrance ramps that were previously used as exit ramps during non-contraflow travel. Since the VC system can easily monitor traffic flow, it could offer recommendations to the emergency center about which roadways are good contraflow candidates.

19.8.4 Unplanned Evacuation Management

To date, there has been more of a focus on the analysis and planning of events where some notice is provided than for no-notice events [57]. When advance notice is provided, agencies have an opportunity to set up traffic control to facilitate outbound movements. The advance notice cases usually involve a known potential threat, such as a hurricane, and a known response to that threat. In contrast, in the case of *unplanned evacuations*, little or no prior notice is possible since such evacuations are set up in response to an unpredictable event such as a hazardous material spill, a terrorist attack, and the like. Detailed pre-planning for no-notice events is much more difficult since infinite possibilities for the location and type of event are possible. Thus, modeling large-scale no-notice events is based on a considerable number of assumptions that may or may not actually represent a real event response. Assumptions on how travelers will behave, as well as the nature of an event, in the case of a no-notice evacuation can have a significant impact on the model results.

Several studies have discussed the impact of behavioral assumptions on no-notice evacuation scenarios. Recently, Lindell and Prater [58] examined behavioral assumptions that need to be considered in hurricane evacuation planning. They noted the need to improve the quality of data collected through surveys, and they also pointed out that more data on route choice, departure time, and other factors influencing evacuation decision, route choice, and timing are needed. Litman [45] examined lessons learned from Hurricanes Katrina and Rita, and he assessed areas where evacuation plans fell short. He noted that there was an overall underestimation of the number

of evacuees, along with a failure to account for transit-dependent populations. Behavioral assumptions are even more important in the case of no-notice evacuations. Murray-Tuite and Mahmassani [46] examined transportation impacts of families gathering together prior to evacuating. They found that failure to account for this behavior could result in overly optimistic predictions of evacuation travel times.

The number of uncertainties in no-notice evacuation models limits the direct applicability of pre-analyzed scenarios in the event that an actual evacuation occurs. Ideally, agencies would have the capability to develop and modify plans based on analysis as the event unfolds, rather than simply reacting after conditions have already broken down. However, the complexity and analysis time of existing models makes this very difficult. For example, due to the size and complexity of the network, a recent hurricane evacuation analysis by Edara and McGhee [44] took 36 hours of computation time to simulate a 24-hour evacuation scenario. In contrast, the huge computational power in the thousands of evacuating vehicles could offer an opportunity to develop near-real-time route recommendations and traffic control responses in response to an evacuation event. This would allow for explicit consideration of factors like time of departure, observed route choice, and location and nature of the event causing the evacuation.

19.8.5 Sharing On-Road Safety Messages

The trend in the car manufacturing industry is to equip new vehicles with major sensing capabilities in order to achieve efficient and safe operation. For example, Honda is already installing cameras on their Civic models in Japan. The cameras track the lines on the road and help the driver stays in lane. A vehicle would thus be a mobile sensor node and an VC can be envisioned as a huge wireless sensor network with very dynamic membership. It would be beneficial for a vehicle to query the sensors of other vehicle in the vicinity in order to increase the fidelity of its own sensed data, get an assessment of the road conditions and the existence of potential hazard ahead. For example, when the tire pressure sensor on a vehicle reports the loss of air, vehicles that are coming behind on the same lane should suspect the existence of nails on the road and may consider changing the lane. The same happens when a vehicle changes lane frequently and significantly exceeds the speed limit; vehicles that come behind, and which cannot see this vehicle, can suspect the presence of aggressive drivers on the road and consider staying away from the lanes and/or keeping a distance from the potentially dangerous driver. The same applies when detecting holes, unmarked speed breakers, black ice, and so on. Contemporary VANET design cannot pull together the required solution and foster the level of coordination needed for providing these safety measures.

19.8.6 Autonomous Mitigation of Recurring Congestion

In face of traffic congestion, some drivers often pursue detours and alternate routes that often involve local roads. Making the decision behind the steering wheel is often challenging. The driver does not know whether the congestion is about to ease or

is worsening. In addition, when many vehicles decide to execute the same travel plan, local roads become flooded with traffic that exceeds its capacity and sometimes deadlocks take place. Contemporary ITS and traffic advisory schemes are both slow to report traffic problems and usually do not provide any mitigation plan. A VC-based solution will be the most appropriate and effective choice. Basically, vehicles in the vicinity will be able to query the plan of each other and estimate the impact on local roads. In addition, an accurate assessment of the cause of the congestion and traffic flow can be made by contacting vehicles close to where the bottleneck is. In addition, appropriate safety precautions can be applied to cope with the incident, e.g., poor air quality due to the smoke of a burned vehicle.

Interestingly, this approach can be applied not to drivers on the road but also to those who are about to leave home. Delayed start and telecommuting may be considered as an alternative in order to increase productivity and avoid wasted energy and time.

19.8.7 Dynamic Management of Parking Facilities

Anyone who has attempted to find a convenient parking spot in the downtown area of a big city or close to a university campus where the need for parking by far outstrips the supply would certainly be interested to enlist the help of an automated parking management facility. The problem of managing parking availability is a ubiquitous and a pervasive one, and several solutions were reported recently [59,60]. However, most of the known solutions rely on a centralized approach where reports from individual parking garages and parking meters are aggregated at a central, citywide location and then disseminated to the public. The difficulty is with the real-time management of parking availability since the information that reaches the public is often stale and outdated. This, in turn, may worsen the situations especially when a large number of drivers are trying to park, say, to attend a downtown event.

We envision that by real-time pooling the information about the availability of parking at various locations inside the city, a VC consisting of the vehicles that happen to be in a certain neighborhood will be able to maintain real-time information about the availability of parking and direct the drivers to the most promising location where parking is (still) available.

19.8.8 Homeland Security Applications

Sensor networks are expected to evolve into long-lived, open, ubiquitous, multipurpose networked systems. Recently, Eltoweissy et al. [61] have proposed ANSWER, an autonomous networked sensor system whose mission is to provide in situ users with real-time, secure information that enhances their situational and location awareness. ANSWER finds immediate applications to homeland security. The architectural model of ANSWER is composed of a large number of sensors and of a set of (mobile) aggregation-and-forwarding nodes, possibly VC nodes, that organize and manage the sensors in their vicinity. As argued in reference 61, ANSWER can provide secure, QoS-aware information and analysis services to in situ mobile users in support of application-level tasks and queries while hiding network-level details. We anticipate

that a VC can naturally interface in a symbiotic relationship with ANSWER, creating a powerful mission-oriented system.

As a second possible homeland security application, we look at the efficient tasking of law enforcement officers. It is well known that law enforcement officers play a crucial role in keeping the roadways and street safe for the traveling public. Even if a police vehicle is so visible on the road, it serves as a deterrent for aggressive drivers and vehicle safety violators. A VC can be used as an effective resource-planning tool for the police squad. Moving vehicles form a VC and report to the police so that decisions can be made efficiently about deploying troopers in certain spots and/or employing surveillance cameras and aircraft to identify and videotape violators for further assigning fines. That will allow effective usage of officers' time and enable them to allocate resources for other vital tasks such as criminal investigation and prevention. Implementing this idea using state-of-the-art technology is resource prohibitive and requires major infrastructure investment.

19.8.9 Vehicular Clouds in Developing Countries

We conjecture that the usefulness and practicality of the VC concept will become even more apparent in developing countries lacking a sophisticated centralized decision-support infrastructure. We further conjecture that, in such contexts, VCs will play an essential role in bringing together a huge number of relatively modest computational resources available in the vehicular network into one or several foci of computing and communications that will find and/or recommend solutions to problems arising dynamically and that cannot possibly be resolved with the existing infrastructure. We have seen a similar phenomenon happening with the penetration of cell phones in developing countries where they were adopted rapidly and unhesitatingly by a population that had access to a modest land-line telephony system.

19.9 SECURITY AND PRIVACY IN VEHICULAR CLOUDS

In this section we are interested in identifying and analyzing a number of security challenges and potential privacy threats in VCs. We address some major design issues that will affect the future implementation of VC and provide a set of security and privacy-preserving protocols. Many of the security challenges have received attention in related fields such as cloud computing and VANET. However, our goal is to address *unique security challenges* exacerbated by features specific to VCs—for example, the challenges of authentication of high-mobility vehicles and the complexity of trust relationships among multiple players caused by intermittent short-range communication.

19.9.1 Overview

Recently, a great deal of attention has been devoted to the general security problem in clouds, although not associated with vehicular networks [62,63]. The simplest

solution is to restrict access to the cloud hardware facilities. This can minimize risks from insiders [64]. Santos et al. [65] proposed a new platform to achieve trust in conventional clouds. A trust coordinator maintained by an external third party is imported to validate the untrusted cloud manager which makes a set of virtual machine such as Amazon's E2C (i.e., Infrastructure as a Service, IaaS) available to users. This solution focuses on the confidentiality and integrity of data. Garfinkel et al. [66] proposed a solution to prevent the owner of a physical host from accessing and interfering with the services on the host. Berger et al. [67] and Murray et al. [68] have adopted similar solutions. When a virtual machine boots up, system information such as the BIOS, system programs, and all the services applications is recorded and a hash value is generated and transmitted to a third part Trust Center. For every period of time, the system will collect system information of the BIOS, system programs and all the service applications and transmit the hash value of system information to the third party Trust Center. The Trust Center can evaluate the trust value of the cloud. Krautheim [69] also proposed a third party to share the responsibility of security in cloud computing between the service provider and client, decreasing the risk exposure to both. Jensen et al. [70] stated technical security issues of using cloud services on the Internet access. Wang et al. [71,72] proposed public-key-based homomorphic authenticator and random masking to secure cloud data and preserve privacy of public cloud data. The bilinear aggregate signature has been extended to simultaneously audit multiple users. Ristenpart et al. [73] presented experiments of locating co-residence of other users in cloud virtual machines.

In parallel, and independently of cloud security, the topic of VANET security and privacy has been addressed by a large number of researchers in the past decade. Yan et al. [27,28] proposed active and passive location security algorithms. On-board radar devices can be employed as a "virtual eye" since they can detect the location of neighboring vehicles on the road. In particular, the on-board radar device can validate the claimed location of a vehicle, received and computed by GPS receivers. The proposed Public Key Infrastructure (PKI) and digital signature-based methods have been well-explored in VANET [74–77]. A certificate authority (CA) generates public and private keys for nodes. Laberteaux et al. [78] discussed applying a similar method to sign messages in VANET. The purpose of the digital signature is to validate and authenticate the sender. The purpose of encryption is to disclose the content of message only to the nodes with secret keys. PKI is a method well-suited for security purposes, especially for roadside infrastructure, like roadside e-shops, Internet access points, and so on. GeoEncrypt [79,80] in VANET has been proposed by Yan and Olariu [81]. The geographic location of vehicles is used to generate secret keys. Messages are encrypted by the secret keys and the ciphertexts are sent to receiving vehicles. Receiving vehicles must be physically present in a certain geographic region specified by the sender to be able to decrypt the message.

However, the security and privacy research in VCs has not yet been addressed in the literature. It goes without saying that if the VC concept is to see a wide adoption and to have significant societal impact, security and privacy issues in VCs need to be addressed. VC has great potential security and privacy challenges that are different from the conventional wireless networks, VANET, or cloud computing. Conventional

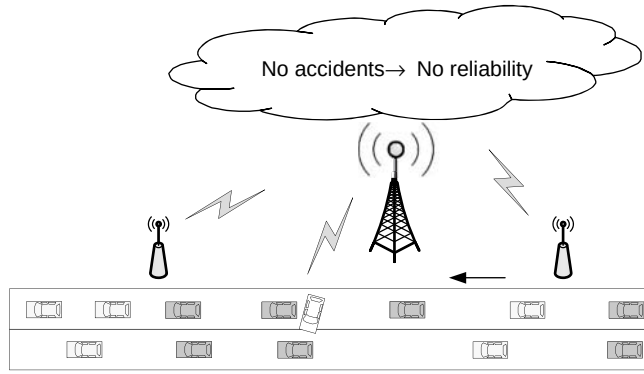

Figure 19.3 Illustrating a security issue in VC.

networks attempt to prevent attackers from entering a system. However, in VC, all the users including the attackers are equal. The attackers and their targets may be physically colocated on one machine. The attackers can utilize system loopholes to reach their goals, such as obtaining confidential information and tampering with the integrity of information and the availability of resources. Figure 19.3 illustrates one possible example of tampering with the integrity of information in the case of a road accident. An accident occurred at an intersection, and the accident will be reported to the VC. The driver who is liable for the accident can invade the VC and modify the accident record. Later, when the law enforcement or the vehicle insurance company query the accident, they cannot link the accident to the driver that caused it.

Even though security and privacy have received a good deal of well-deserved attention in related fields such as wireless networks, cloud computing, and VANET, there are a number of security and privacy issues that are novel in VCs. Similarly, there are numerous security and privacy challenges brought about by the unique features of VC. Compared to cloud computing, the security challenges of VCs have unique facets as well. While the nodes in a conventional cloud are static, the resources in a VC are, as a rule, mobile. It is well-documented that the wireless communications between vehicles are inherently intermittent and mostly short-lived [82]. Since the vehicles communicate mainly through short-range wireless transceivers, the high mobility of vehicles is apt to cause significant challenges related to managing authentication, authorization, and accountability. For example, vehicles are extremely hard to authenticate in real-time, location-specific applications (e.g., collision warning or road condition monitoring). The tradeoffs between security and performance will need to explored. Vehicular mobility will also cause significant challenges related to privacy [83]. For example, in order to preserve privacy, it is imperative to keep the locations visited by a vehicle confidential even if the driver chooses to communicate while on the move. The use of pseudonyms [84] is a common solution, but the high mobility presents difficulties in updating the vehicle's pseudonyms. The short-range communication of vehicles will rely on multihop routing that will involve multiple nodes in the network. The more nodes involved, the more risks to authentication and

authorization. The large population of vehicles and the wide spatial distribution of vehicles cause challenges of maintaining infrastructures as well.

The main topics discussed in this section include: (1) analysis of security challenges and privacy threats in VC, (2) discussion of major design issues that will affect the implementation of VC, and (3) a set of security protocols and solutions to enhance security and protect privacy in VCs.

19.9.2 The Attacker Model

Traditional security systems are often designed to prevent attackers from entering the system. However, security systems in CC have a much harder time to keep attackers at bay because multiple service users can share the same physical infrastructure. In the VC environment, attacks can equally share the same physical machine/infrastructure as their targets, although both of them are assigned with different virtual machines. To this point, attackers can have more advantages than the attackers on the traditional system. On the other hand, attackers have challenges. They need to determine on which computer a victim is physically executing programs. It is challenging because all users are randomly assigned to VMs. But it is possible to locate the co-residence of other users. Experiments have been done to catch and compare memory of processors, and users can find co-residence in the same physical machine [73]. Therefore, the attacker model is defined as follows:

- VC cloud infrastructure is a trusted entity.
- VC service providers are trustworthy.
- The vast majority of VC users are trustworthy.
- The attackers are (malicious) users who enjoy the same privileges that normal users do.

The main targets of an attack are:

- Confidentiality, such as identities of other users, valuable data and documents stored on VC, and the location of the virtual machines (VMs) where the target's services are executing.
- Integrity, such as valuable data and documents stored on VC, executable code and result on VC.
- Availability, such as physical machines and resources, services, and applications.

There are several challenges for attackers. First, the attackers must find out the location where the target user's services are executing. Second, the attackers must physically colocate with the target user on the same physical machines. Finally, the attackers have to collect the valuable information with certain privileges.

One possible form of attack is the following:

- Narrow down the possible areas where the target user's services are executing by mapping the topology of VC.

- Launch multiple experimental accesses to the cloud and find out if the target user is currently on the same VM.
- Request the services on the same VM where the target user is on.
- Using the system leakage to obtain higher privilege to collect the assets [73].

19.9.3 Taxonomy of Threats

The threats in VC can be classified on the basis of STRIDE [85], which is a system developed by Microsoft for classifying computer security threats. The threat categories are:

- *Spoofing User Identity*. The attacker pretends to be another user to obtain data and illegitimate advantages. One classic example is "man-in-the-middle attack" in which the attackers pretend to be Bob when communicating with Alice and pretend to be Alice when communicating with Bob. Both Alice an Bob will send decryptable messages to the attackers. An other example is similar "email address spoofing" in which the attackers fill with forged return user's identity and create errors of unreachable bounces.
- *Tampering*. The attacker alters data, modify and forge information.
- *Repudiation*. The attacker manipulates or forges the identification of new data, actions and operations. Repudiation means data manipulation in the name of other users.
- *Information Disclosure (Privacy Breach or Data Leak)*. The attacker uncovers personally identifiable information such as identities, medical, legality, finance, political, residence and geographic records, biological traits, ethnicity, etc.
- *Denial of Service (DoS)*. The attacker takes a series of seemingly bona fide actions that, however, consume an inordinate amount of system resources and make the resources unavailable to legitimate users.
- *Elevation of Privilege*. The attacker exploits a bug, system leakage, design flaw, or configuration mistake in an operating system or software applications to obtain elevated access privilege to protected resources or data that are normally protected from normal users. The attacker then can access the protected data with higher or more privileges that are often assigned to administrators or coordinators.

19.9.4 Trust Relationship

Trust is one of the key factors in any secure system [86]. A trust relationship can exist in several ways. The network service providers and the vehicle drivers have access trust. There will be a large amount of government agents—for example, the Department of Motor Vehicles (DMV) and the Bureau of Motor Vehicles (BMV)—as trusted entities. The relationship between BMV and vehicle drivers is identity uniqueness and legitimacy.

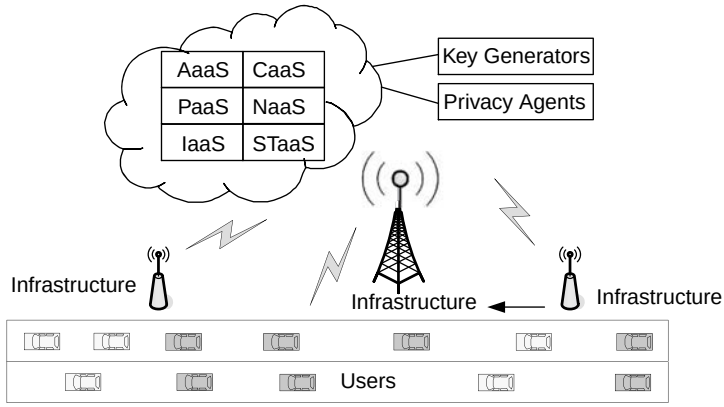

Figure 19.4 Multiple participants in a VC. Vehicles often communicate through multihop routing. A request response will include multiple participants including users, infrastructure, servers, platform, application, key generator, and privacy agent.

However, the large population of vehicles creates challenges to building trust relationships to all the vehicles at any time. There will be occasional exceptions. In addition, drivers are increasingly concerned about their privacy. Tracking vehicles/drivers will cause worries in most cases. As a result, pseudonyms are often applied to vehicles. On the other hand, a certain level of trust is needed. Some applications such as accident liability investigation by law enforcement or insurance require driver's identity to be responsible to accidents. Therefore, we assume a low level of trust relationship exists in VANETs.

In a VC, it is actually far more challenging to build trust relationship because there are more participants than VANETs and conventional cloud computing. Figure 19.4 shows an example of multiple participants in VC. VC is often based on short-range wireless communication. Many applications will need multihop routing. Multiple nodes will be involved in VC communication. Therefore, VC has inherited the challenge of establishing trust relationship among multiple vehicles, roadside infrastructure, service provider, network channels, and even the secret key generator.

19.9.5 Authentication of High-Mobility Nodes

The security authentication in VC includes verifying a user identity, message integrity, and checking the integrity of a transmitted message. To conduct authentication, there are some conventional ways [87] such as:

- *Ownership*. A user owns some unique identity (e.g., Identity Card, security token, software token).
- *Knowledge*. A user know some unique things (e.g., passwords, personal identification number, human challenge response (i.e., security questions)).
- *Biometrics*. Signature, face, voice, fingerprint.

However, the VC environment is different from conventional clouds and networks. Vehicles, the nodes of the VC, are mobile and often register once a year with the Department of Motor Vehicles (DMV) or with the Bureau of Motor Vehicles (BMV). This imposes significant difficulties and challenges of authentication. For example, accident alert message associated with vehicular locations and events at a specified time can be hard to verify because the locations of vehicles are constantly changing. Even the identity of drivers are hard to authenticate as well because drivers' identities are protected for the sake of privacy. Vehicles cannot tell the identities of drivers who are operating them.

19.9.6 VC Messages

19.9.6.1 Safety Messages. The initial motivation of VANETs was to support safety applications. Safety-related messages are major information in the network. Based on the emergency level, there are three types of safety messages:

- Level one, public traffic condition information. Vehicles switch traffic information (e.g., traffic jam) that indirectly affects other vehicles' safety as traffic jam will increase the likelihood of accidents. This type of message is not sensitive to communication delay, but privacy needs to be protected.
- Level two, cooperative safety messages. Vehicles exchange messages in cooperative accident avoidance applications. These messages are bounded by a certain time range (normally people think it is real-time communication), and privacy needs to be protected.
- Level three, liability messages. After accidents occur, there will be liability messages generated by law enforcement or authorities. These messages are important evidence for liability claim and are bonded by a certain time range. Privacy information is naturally protected.

A common format of safety messages can be defined as follows: timestamp, geographic position, speed, percentage of speed change since last message, direction, acceleration, and percentage of acceleration change since last message. The safety message will append information such as public traffic condition, accidents, and so on. The appended message can help to determine liability. Driver identity information is not necessary to be part of the safety message. Pseudonyms can be applied to protect the driver's identity.

The signature of safety messages can be described as follows. Following ElGamal signature scheme [88], we define parameters:

- Let H be a collision-free hash function.
- Let p be a large prime. This number will ensure that computing discrete logarithms modulo p is very difficult.
- Let $g < p$ be a randomly chosen generator out of a multiplicative group of integers modulo p.

Each vehicle has long-term PKI public/private key pairs:

- Private key: S
- Public key: $< g, p, T >$, where $T = g^S \bmod p$

It should be noted that m can be $m|T$ where T is the timestamp. The timestamp can ensure the freshness of the message. For each message m to be signed:

- Generate a per-message public/private key pair:
  Private: S_m
  Public: $T_m = g^{S_m} \bmod p$
- Compute the message digest: $d_m = H(m|T_m)$
- Compute the message signature: $X = S_m + d_m S \bmod(p-1)$
- Send: m, T_m, and X

where mod is the modulo operation, | is the concatenation operator.

To verify the message, three steps are needed:

- Compute the message digest: $d_m = H(m|T_m)$
- Compute: $Y_1 = g^X$ and $Y_2 = T_m T^{d_m}$
- Compare $Y_1 = Y_2$. If $Y_1 = Y_2$, then the signature is correct.

The reason:

$$Y_1 = g^X = g^{S_m + d_m S} = g^{S_m} g^{d_m S} = T_m g^{S d_m} = T_m T^{d_m} = Y2$$

19.9.6.2 Confidential Messages. To ensure the confidentiality of sensitive message, the message will be both signed and encrypted. Suppose vehicle A sends a sensitive message m to vehicle B. Each vehicle has its own PKI public/private key pairs. Thinking of the overhead of PKI processing time, we can adapt symmetric encryption algorithm. But to exchange the secret key, we still need to use PKI support. The handshake of exchanging the secret key is defined as follows:

$$A \rightarrow B : B|K|T_{pub_B}, SigB|K|T_{pri_A}$$

where A and B are the identities of vehicle A and B, K is the secret key shared by A and B, m is the sensitive message, T is the timestamp, pub_B is the public key of B, and pri_A is the private key of A.

Once A and B both know the secret key K, A and B can communicate by using a well-known message authentication code (MAC or HMAC) in cryptography. Hashing the sensitive message as shown follows:

$$A \leftrightarrow B : m, MAC_K m$$

There are potential problems with this approach. As a drawback of symmetric encryption, nonrepudiation (i.e., integrity and origin of data) cannot be ensured, although the likelihood of data being undetectably changed is extremely low. This is a compromised solution between efficiency and security. To achieve higher-level security of a sensitive message, one can apply an active security mechanism [27] or adopt PKI encryption at a cost of losing certain amount of efficiency. Given the fact that VANETs are multihop networks, the key handshake in this scheme does not scale well in pure autonomous/adhoc VANETs. But it can scale well with the aid of roadside infrastructure.

19.9.7 The Requirements

A secure VC should meet the following requirements:

- *Integrity*. Messages should not be tampered with or modified. The messages must be reliable and valid.
- *Confidentiality*. Sensitive messages should not be disclosed by unauthorized users.
- *Availability*. Messages should be available whenever they are needed.
- *Authentication*. Messages must be sent in a legitimate mode and by authorized nodes. We will authenticate both the sender legitimacy and the content of messages.
- *Anti-DoS*. The VC should be able to prevent DoS attacks.
- *Real-Time Constraints*. Some applications, such as accident alerts, require real-time or near real-time communication.
- *Privacy*. The user's privacy should be preserved.
- *Sybil Attack-Free*. Messages sent by unauthenticated parties should not be transmitted.

19.9.8 Data Isolation and Sanitization

Data are shared by the vehicles that participate in the VC. Traffic congestion information is reported to the VC and redistributed by all vehicles in the VC. Traffic accident data are also reported by vehicles or polices in the VC. Records such as arrest records, liability report, and criminal data would be vulnerable when the sensitive data are stored and maintained on ordinary virtual machines. Therefore, data must be stored and accessed securely. Sensitive data need to be isolated from publicly accessible data and to be stored in encrypted form and at physically separated devices and locations. Access to sensitive data will be strictly authenticated and identity-based. Sensitive data must be secured in storage, transit, and use. Encryption to sensitive data will be utilized in almost all transmission protocol.

Sanitization of sensitive data is also important in VC. The devices that store, transit, and use sensitive data need to be specially processed to remove sensitive data from these devices. In VC, a virtual machine can assign a physical device that has

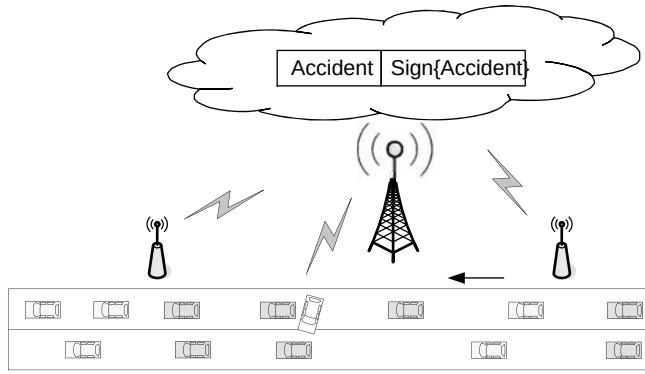

Figure 19.5 A VC security example.

been used to store sensitive data to an attacker. With a proper software and special skills, the sensitive data can be restored from the device. Some instances have been found that sensitive data can be collected from auctioned computer machines that used by organizations such as hospitals, government agents, or law enforcement [89]. For example, repeatedly formatting storage devices and rewriting garbage data many times can be a good practice of hard disk sanitization.

19.9.9 Digital Signatures

Applications that do not contain sensitive messages but require integrity can apply digital signature. Confidentiality is not required because of no sensitive messages included. Therefore, the messages will be authenticated but not encrypted. For example, accident alert application will not include sensitive message but require the integrity of the message. The message can be signed and attached to the original message as illustrated in Figure 19.5.

There are two ways to sign a message: symmetric algorithm and asymmetric algorithm. The advantage of symmetric algorithm is time efficiency. Symmetric algorithms are normally faster than asymmetric ones. However, normally secret key management is a challenging task, given the population of vehicles. The handshake to establish a secret key needs extra overhead as well. Asymmetric algorithms do not require the handshake process. Normally the public key is well known or easier to be known. As a widely adapted asymmetric algorithm, Public Key Infrastructure (PKI) is a suitable asymmetric algorithm for the VC.

19.9.10 Encryption

Messages in VC can include sensitive information. To protect confidentiality of sensitive information, messages can be encrypted. There are multiple ways to encrypt messages. The simple ones include XOR, Caesar cipher, and so on. There are two categories of widely used algorithms: symmetric algorithm and asymmetric algorithm. Normally, PKI will be a suitable solution, especially for infrastructure based the VC.

19.9.11 Authentication

Authentication is a process whereby the VC verifies that someone is who they claim to be or by which the VC verifies the message content as claimed. There are multiple ways to authenticate the users or the message content. For example, we can use digital signature to authenticate the messages and use the MD5 hash algorithm to authenticate the sender's identity.

19.9.12 Authorization or Access Control

Authorization or access control is finding out if a user is permitted to access (e.g., read, write) the resource after it is identified. This is often determined by finding out if that user is a part of a particular group, if that user has owned admission, or if that user has a particular level of security clearance. Users in VC will have particular roles. Each role is associated with a certain access privileges to some resources.

19.9.13 Location Validation

Most, if not all, applications in VC rely on accurate and valid location information. Therefore, location information must be validated. There are two approaches to validate location information: active and passive. Vehicles or infrastructure with radar (or camera, etc.) can perform active location validation. The location measurement of radar can validate the claimed location. Vehicles or infrastructure without radar, or in a situation that radar detection is not within line of sight, can validate location information by applying statistical methods.

19.9.14 Validation of User Identity

Besides digital signature and hash algorithms, user's identity can be validated by using physical locations. In wireless communication, user's location can be detected and validated by using wireless signal strength.

19.9.15 Puzzle Check and Resource Verification

In VC, puzzles can be used to validate users as well. To prevent fake message with manipulated user identity or IP address, a simple puzzle can be sent. A puzzle example can be: What are the last three letters sent in the last message?

19.9.16 Anti-Tamper Devices and Algorithms

Messages can be saved on vehicles' storage. If the message include sensitive material, the message can be saved in anti-tamper devices and encrypted with suitable algorithms.

19.9.17 Throttling and Filtering

VC is based on wireless networks. The network attacks and virus can be controlled by attack throttling and filtering in infrastructure-based VC. A normal application can connect a network node with a certain rate. An application that is mounting an attack will normally connect other nodes with a high rate to spread out virus to find more targets. Attack-throttling or attack-filtering is to put a rate limit on connections to new nodes. In this way, normal traffic remains unaffected but suspect traffic that attempts to spread faster than the allowed rate will be slowed or shut down.

19.9.18 Pseudonymization

VC includes applications that include privacy information. To protect privacy, one can replace a temporal identity assigned by VC as a pseudonym. The real identity can only be discovered by a Pseudonymization Service center which is secured by authority and trusted by all users. The pseudonym is subject to timeout. After expiration time, a new pseudonym will be assigned.

19.9.19 System Maintenance

To reduce the risk of system holes, VC system needs to update the system utilizes periodically and to turn off all the unnecessary services and applications.

19.10 KEY MANAGEMENT

There are two types of cryptographic information: identity information and key information. Many types of information can be identities, but identities used in this chapter must be unique and verifiable. For example, liability-related applications (e.g., insurance investigation after accidents) will normally need identities. Digital License Plate or Electronic License Plate, which is a wireless device broadcasting unique identity string periodically, has been proposed [86]. Since privacy is also considered, keys will not release the identities, so called anonymous keys. Public key can serve as identity as well [77].

In cryptography (more specifically PKI), there are important entities that issue digital certificates. These entities are often called Certification Authority (CA).

19.10.1 Anonymous Keys

Tracking vehicles causes concerns and worries of drivers in VANET. PKI may expose vehicle's identity to attackers. Therefore, it is important to provide anonymous keys. Vehicle's identity includes not only Digital License Plate or Electronic License Plate but also IP address, MAC address of network interfaces. Therefore, the identity information needs to be replaced from time to time. And the "long-term" PKI public key can be tracked, although there is no relationship between the public key and the

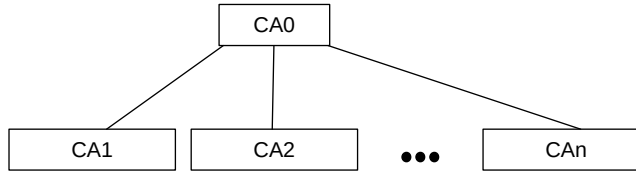

Figure 19.6 CA structure. Flat-structure CAs ensures that issue digital certificates to local vehicles.

driver's identity. A driver's location can be tracked as well. Therefore, the anonymous keys should be changed in a way that most attackers cannot track the vehicle. A possible solution has been proposed by Raya [86].

19.10.2 Key Assignment and Re-keying

In VANET, some organizations can serve as CA: (1) *Governmental Transportation Authorities.* Vehicles are actually registered in DMV or BMV and vehicles are required to perform state-check to issue new permission. These governmental authorities are ideal agents to serve as CA. Key pairs are issued by DMV/BMV and are renewed every year. The vehicular maintenance habits of drivers will not be changed and drivers will not be forced to conduct other actions to get their car certificated. There is a potential problem that vehicles are often registered and state-check are renewed at local agents instead of a centralized agent. Each local agent receives certificates from the higher-level agent. A possible solution is to make a CA chain that includes several levels of CAs. Each of them has a series of CAs as shown in Figures 19.6 and 19.7. A tree structure can be organized as shown in Figure 19.7.

(2) *Vehicle Manufacturers.* Manufacturers will receive permission and certificates from governmental transportation authorities and become a subdivision of CA. (3) Nonprofit organizations. Similar to vehicle manufacturers, nonprofit organizations can obtain permission and certificates from governmental transportation authorities and become a subdivision of a CA.

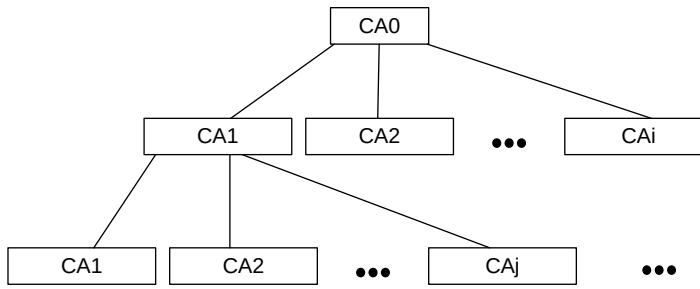

Figure 19.7 CA structure. Tree-structure CAs ensures that issue digital certificates to local vehicles.

Vehicles can be assigned key pairs in VC. Initially, a vehicle will receive a key pair from manufacture or governmental transportation authorities. Key assignment is on the basis of the unique ID and a certain expiration time. The key pair has to be periodically renewed at local DMV/BMV served as sub-CAs when the expiration time is up. The renew/expiration period can be the same period of vehicular state check—for example, annual state-check in many US states.

19.10.3 Key Verification

To verify key pairs, we assume the following:

- Every vehicle trusts the CA.
- CAs are tamper-proof.

Key validation can be done at the CAs or sub-CAs. Let pub_i of a vehicle i be the public key issued by a CA j, that is, CA_j. The vehicle i will have a certificate $cert_i[pub_i]$ assigned by CA_j when CA_j assigns the public key. The process of validating public key will compute the following certificate at CA_j:

$$cert_i[pub_i] = pub_i | sig_{pri_{CA_j}}(pub_i | ID_{CA_j})$$

where pri_{CA_j} is the private key of CA_j and ID_{CA_j} is the identity of CA_j. The idea is to sign the special message $pub_i | ID_{CA_j}$ using the private key of CA_j and the digital signature algorithm has been discussed in Section 19.9.6.1.

19.10.4 Key Revocation

Key revocation is one of the important and effective ways to prevent attacks and to mitigate their effect. There are certain cases that key pairs will be exposed to attackers. It is obvious that the exposed key pair needs to be disabled. One of the advantages of PKI is that PKI can revoke a key pair. Vehicles will be aware that the exposed key pair has been revoked and refuses to communicate with vehicles with invalid key pairs. PKI uses Certificate Revocation Lists (CRL) to revoke keys. CRL includes a list of the most recently revoked certificates and are instantly distributed to vehicles. In VANET, the infrastructure can serve as CRL distributors.

CAs can revoke key pairs by using on-board tamper-proofed devices [90]. Suppose CAs want to revoke the key pairs of a vehicle V. CAs will send out the revoke message signed by public key of V to the tamper-proofed devices. After receiving this revocation message, the tamper-proof device will validate the message and revoke the key pairs. The tamper-proof device will also send back ACK to the CA to confirm the operation. To improve communication between V and CA, vehicle's location is retrieved to select the closest CA. If the latest vehicle location cannot be retrieved, the last location will be used to select the closest CA. In this case, CA will use a broadcast message to revoke the key pairs. The broadcast message can be sent out by using several media such as FM, Internet, satellite, and so on.

To avoid anti-social attackers reporting other vehicles to CA to revoke the key pairs of other vehicles, revocation will be triggered by a certain amount of neighboring vehicles. There is another risk that attackers can launch planned attacks. For example, several attackers can surround a well-behaved vehicle and report the well-behaved vehicle as a misbehaving vehicle. This risk is very challenging to prevent. Thanks to the dynamics of traffic, it is costly to launch such an attack. One possible solution is to build behavior history records and credit the past behavior into values, just like the bank credit system. Similar solution has been discussed as "Map History" [27]. CRL can refer the credit value to perform revocation.

19.11 RESEARCH CHALLENGES

The application scenarios discusses above require better V2V and V2I collaboration in order to reach critical and mutually beneficial decisions, effective and unconventional management to cope with the highly dynamic nature of the computing, communication, sensing, and physical resources, and well-defined operation structures that enable autonomy and authority in adjusting local settings with the potential of making wide impact. Vehicular clouds are complex entities that must be designed and engineered to withstand structural stresses induced by the inherent instability in the operating environment. A VC is defined by its aggregated cyber-physical resources; their aggregation, coordination, and control are facing nontrivial research challenges, as outlined below.

- *Architectural Challenges*. These challenges include issues related to the organization of the logical structure of the VC and its interaction with the physical resources; there is a critical need manage efficiently host mobility and heterogeneity (including computing, communication and storage capabilities) and vehicle membership (change in interest or location, resource denial, failure, etc.).
- *Security and Functional Challenges*. In order for the VC vision to become reality, the problems of assuring emergent trust and security in VC communication and information need to be addressed. The establishment of trust relationships between the various players is a key component of trustworthy computation and communication. Since some of the vehicles involved in a VC may have met before, the task of establishing proactively a basic trust relationship between vehicles is possible and may be even desirable (think in terms of vehicles that "meet" day after day in a parking garage). Research is needed on developing a trustworthy base, negotiation and strategy formulation methodology (e.g., game theory), efficient communication protocols, data processing, and so on.
- *Operational and Policy Challenges*. In order for the VC to operate seamlessly, issues related to authority establishment and management, decision support and control structure, the establishment of incentives, accountability metrics, assessment and intervention strategies, rules and regulations, standardization, and so on, must all be addressed. Dealing with these issues requires a broad participation that must involve local, state and/or federal decision makers. By the same

token, there is a need for economic models and metrics to determine reasonable pricing and billing for VC services.

19.12 ARCHITECTURES FOR VEHICULAR CLOUDS

Although our ultimate goal is to produce a unified architectural framework for the VC, the main goal of this section is to review several possible architectures, of increasing complexity that suit various particular manifestations of VCs.

19.12.1 A Static Architecture

In some cases, an VC may behave just as a conventional cloud. This is, no doubt, the case in static environments as the one we contemplate below. Indeed, consider a small business employing about 250 people and specializing in offering IT support and services. It is not hard to imagine that, even if we allow for car-pooling, there will be up to 150 vehicles parked in the company's parking lot. Day in and day out, the computational resources in those vehicles are sitting idle.

The company may proactively seek the formation of a static VC by providing appropriate incentives to its employees who will rent the resources of their vehicles to the company on a per-day, per-week or per-month basis. The resulting (more or less) static VC will harvest the corporate computational and storage resources of the participating vehicles sitting in the parking lot for the purpose of creating a computer cluster and a huge distributed data storage facility that, with proper security safeguards in place, will turn out to be an important asset that the company cannot afford to waste.

In the scenario above, the architecture of the VC will be almost identical to the architecture of a conventional cloud, with the additional twist of, perhaps, limiting the interaction to weekdays.

19.12.2 Interfacing with a Static Infrastructure

It is often the case that an VC is created and evolves in an area instrumented by the deployment of some form of a static infrastructure supportive of the management of various activities. In an urban setting, such an infrastructure includes traffic lights, cameras, and the utility or street lighting poles. On our roadways, the static infrastructure includes ILDs, the roadside units, and other ITS hardware deployed in support of traffic monitoring and management.

We note here that in a not-so-distant future, a pre-deployed set of tiny sensors, even if not organized in a permanent sensor network, may play the role of the static infrastructure that the VC may find it beneficial to interact with. In fact, this view is consistent with ANSWER [61] where the place of the PSAR is taken by the VC that is constantly interacting with the static infrastructure.

It is self-evident that the VC benefits from the interaction with the existing static infrastructure. Consider, for example, a city block where a minor traffic-related event has occurred and where, as a consequence, a number of vehicles are colocated. Once

the traffic event has been cleared, relying on the existing scheduling of the traffic lights will not help dissipate the traffic backlog in an efficient way. We envision a solution to this problem where the vehicles themselves will pool their computational resources together, creating the effect of a powerful super-computer that will recommend to a higher authority a way of rescheduling the traffic lights that will serve the purpose of decongesting the afflicted area as fast as possible.

It is worth noting that in this particular instance, the scope of the traffic lights to reschedule is relatively modest and does not require the federation of several VCs.

19.12.3 A Simple Dynamic Architecture

Consider, for example, a city block where a minor traffic-related event has occurred and where, as a consequence, a number of vehicles are colocated. Once the traffic event has been cleared, relying on the existing scheduling of the traffic lights will not help dissipate the traffic backlog in an efficient way. We envision a solution to this problem where the vehicles themselves will pool their computational resources together, creating the effect of a powerful super-computer that will recommend to a higher authority a way of rescheduling the traffic lights that will serve the purpose of decongesting the afflicted area as fast as possible.

It is worth noting that in this particular instance, the scope of the traffic lights to reschedule is relatively modest and does not require the federation of several Arcs. The architecture that will support the formation of this VC will involve the following elements: a broker elected spontaneously among the vehicles that will attempt to spontaneously form an VC. The broker will then secure a preliminary authorization from a higher (city) authority for the formation of an VC. If several brokers attempt to secure such an authorization simultaneously, one will succeed and the others will possibly form a team that will coordinate the formation of the VC. In the sequel we assume that there is a unique broker. The broker will inform the vehicles in the area of the received authorization and will invite participation in the VC. The cars will/or will not respond to the invitation on a purely autonomous basis. The broker decides if a sufficient number of vehicles have volunteered and will then announce the formation of the VC. The VC will pool their computational resources to form a powerful supercomputer that, using a digital map of the area, will produce a proposal schedule to the higher (city) forum for approval and implementation. Once the proposal has been accepted and implemented, the VC is dissolved.

While the scenario above and the resulting architecture are more complex than that of a conventional cloud, we note that, in general, the solution cannot involve only a handful of traffic light but will require rescheduling the traffic lights in a large area. This motivates the collaboration of several VCs.

19.12.4 Security and Functional Challenges

19.12.4.1 Key Management. Securing keys are extremely important in a VC environment. Most security and privacy solutions rely on secret keys or PKI. Unlike centralized systems, a VC is decentralized. Another challenge is the large population

of vehicles which have high mobility. On the other hand, the fact that all vehicles are supposed to be registered and managed by Department of Motor Vehicles (DMV) or Bureau of Motor Vehicles (BMV) can be utilized to distribute and update secret keys. Car manufacturers can distribute initial secret keys as well.

Group keys can be created to secure communication in a group of vehicles. A group leader will be elected and represents all the members in the group. The algorithm that can effectively elect the group leader and secure the communication is challenging. In addition, the methods that efficiently assign and manage the secret keys are also challenging problems.

19.12.4.2 Trust Management. In clouds, trust management can be used to aid the automated verification of actions. The verification will check if the actions demonstrate sufficient credentials, irrespective of their actual identity. If a cloud request includes sufficient credentials that are defined by a cloud service, the cloud service will accept the request without authorization of those who actually launched the request. Therefore, clouds or the third party will monitor the behavior of activities and respond accordingly by increasing or decreasing trust value of the clouds.

19.12.4.3 Location Security. Locations of vehicles are very valuable and unique. Many applications and security validations rely on location information. But the security of locations is an open problem. Although GPS receiver can provide location information of vehicles installed the device, the location of other vehicles cannot be validated by GPS receiver. Yan et al. [27,28] proposed active and passive location security in VANETs. But there are more new challenges in vehicular clouds environment—for example, how clouds validate location integrity, how clouds ensure location availability.

19.12.4.4 DoS Prevention. For wireless media, DoS is extremely hard to prevent. There is no valid solution of DoS for autonomous vehicular cloud computing networks. One of the reasons is that all the vehicles are equal. There is no higher level of control to shut down the DoS attacker when the DoS is detected. But we introduced the throttling and filtering solution in infrastructure-based VC. In most of cases, the throttling and filtering can mitigate the damage of DoS attacks.

19.12.4.5 Message Aggregation and Validation. Users with different perspective are interested in different layers of information. Efficient algorithms will aggregate and validate message to represent as much as possible information and consume as few resources as possible.

19.13 RESOURCE AGGREGATION IN VEHICULAR CLOUDS

As we saw before, VCs can be assembled and utilized in scenarios where the vehicles are stationary and/or on the move. The goal of this section is to propose a possible techniques for resource aggregation in VCs. More precisely, two solutions to the

resource aggregation problem are proposed and evaluated. We have implemented one of these solutions and offer some simulation results.

In this section we follow dedicated DSRC terminology:

- The computing capabilities on board a vehicle are referred to as an on-board unit (OBU).
- We also assume the existence of infrastructure (perhaps installed in the traffic lights themselves) that is referred to generically as roadside units (RSU).

Moreover, the VC architecture follows generic CC terminology [38]. Specifically, three entities will be declared: node, cluster, and cloud controller. As in reference 39, the services provided by the VC can be classified as computing, network, and storage. Examples of computing VC services were provided in Section 19.7. The first two instances of computing VC services are to be implemented while the vehicles are stationary or mobile. These two scenarios follow the well-defined model and could be used for IaaS, PaaS, or SaaS services. The third example presented is applicable to situations when multiple vehicles are involved in traffic congestion. It will allow for the participation of each vehicle's OBU toward the determination of an alternative path for escaping the traffic congestion. The node controller software entity will be running on the OBU of each vehicle, the cluster controller entity will run on the RSU, and the cloud controller will be implemented on a higher authority system (a Department of Transportation (DOT) system in this case). Figure 19.8 presents a high-level architectural view of the dynamic traffic-event mitigation cloud as proposed in reference 39. The mobility characteristics (i.e., parked, slow mobility, high mobility) of each of the VC examples determines the underlying networking infrastructure to be utilized. While wireless communications (WiFi, Cellular 3G or 4G, WiMax, DSRC) are the only possibility for mobile scenarios, in the static cases the VC could be able to employ 100-megabit Ethernet, even 1G, or 10G Ethernet connections as suggested in Subsection 19.7.1.

The conventional cloud architecture is built based on the hardware specifications of datacenter servers interconnected with minimum of 1-gigabit Ethernet. The node controllers are to be hosted on multicore, multiprocessor machines, with high-memory density. The required specifications allow for virtualization of the node hosts to provide the virtual machines (VM) to run user services. The different aspect in a VANET

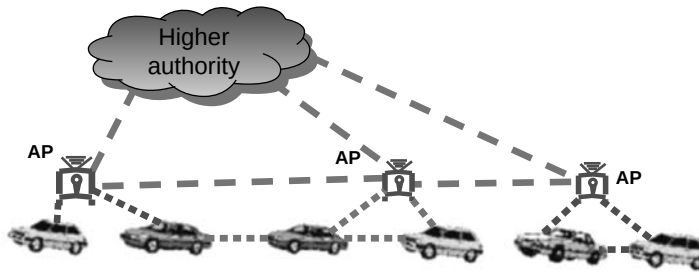

Figure 19.8 A possible VC architecture for dynamic traffic-event mitigation.

environment is the low hardware specifications of embedded OBU units. At this point, the implementation of vehicular computers is expected to have 1-GHz single-core CPU with 1 GB of random access memory (RAM) on average. These computational resources are the limiting factor toward a VC implementation. The current implementation of cloud computing cannot be sustained without the ability of virtualization [91], and thus VCs would require a method of incorporating multiple OBU units towards generating a single VM. The questions to be addressed in this section are: how to aggregate the OBU resources, how to instantiate VMs on the aggregated pools, and what technique to implement in order to deal with OBUs leaving the resource pools.

Two approaches have been proposed, namely, virtualization and load balancing. They will be discussed in Subsections 19.13.1

19.13.1 The Virtualization Approach

The existing virtualization architecture has been presented in Figure 19.9. Three current approaches are para-virtualization, full virtualization, and hardware-assisted virtualization [40,59,67]. All of these methods are built on top of the idea that a hypervisor software will be run on a multiprocessor host that would be controlling multiple VM entities and distributing the available computing resources to them. This architecture is modified to present the VC virtualization architecture in Figure 19.10. In this case, multiple OBUs will be grouped together and a resource schedule entity will be required to organize the incoming and outgoing data. This approach would entail expanding the virtual space of each of the VM processes by adding or subtracting the memory of each new OBU to the general VM memory. The resource schedule would implement a virtual memory management addressing mechanism and send basic blocks of CPU instruction to the appropriate OBU entity. Such current techniques have been utilized by multiple companies and allow for the assembly of a scalable virtualization solution. The main aspect of the functionality of such a system is the memory transfer rate. The average RAM transfer rate is currently 2 to 3 Gbps and is the minimum requirement for a successful VC system. These rates have been

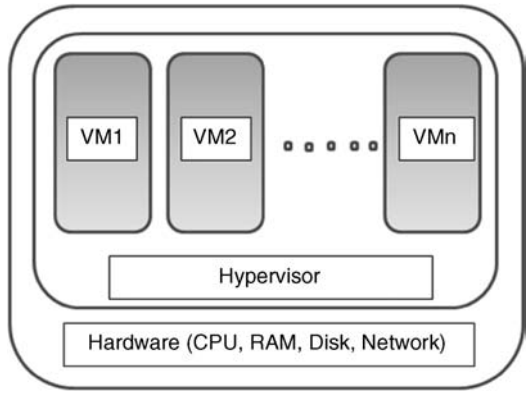

Figure 19.9 Full virtualization.

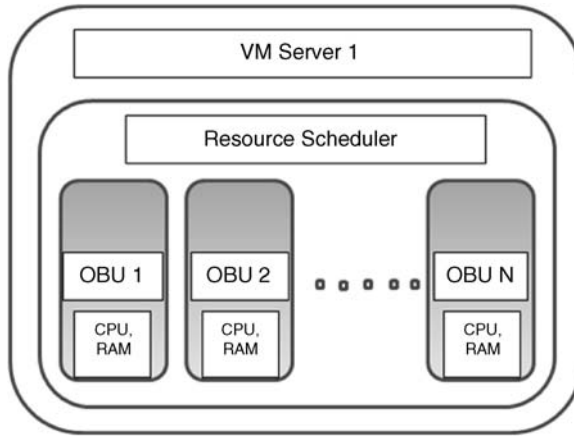

Figure 19.10 OBU virtualization.

so far achieved by a distributed group of systems that use InifiniBand networking to provide these data rates. 40Gbps data rate over the network would allow for 2GBps basic block transfers. Considering the fact that DSRC [92] operates on a 6Mbps data transfer rate, this method of Virtualization is accepted as inapplicable to VC systems.

19.13.2 Load Balancing Approach

A second technique has been proposed as an alternative to our virtualization approach: load balancing [93]. In this section we will concentrate our research on one of the VC scenarios: "Data Center in Your Parking Lot." The overall design of this load balancing VC is presented in Figure 19.11. Figure 19.12 presents a more detailed view of the future architecture of a load-balanced VC. The cluster controller unit on RSU stations will include a load balancing component that will communicate with the node controllers on OBU stations using a wireless medium. This component will register OBUs when vehicles join the cloud and group them as a part of multiple logical VMs as presented in Figure 19.13. The load balancer will maintain records of the member node controllers in a VM, the IP of the VM, and services the VM provides. Each session from a client to a VM will be also monitored, and the cluster controller will make an assignment of incoming requests to available node controllers. An algorithm will be used to determine which VM is most suitable to handle a request. Such algorithms can be selected among random allocation, round-robin, weighted round-robin, and so on.

19.13.2.1 Node Registration. When a vehicle joins the cloud it will initiate communication with the closest RSU (node controller) station. The cluster controller will register the node with a VM instance and send an operating system (OS) image to the node controller. The OS image will be customized to run the required service for that VM. An example of such an image would be a Linux OS distribution running a web server. An average size of an image would be 300 MB, which, including the 120-MB

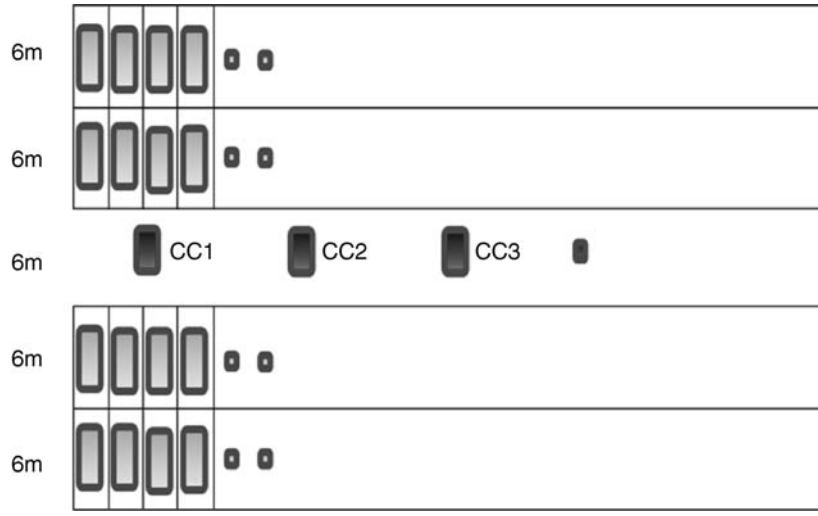

Figure 19.11 A parking lot view.

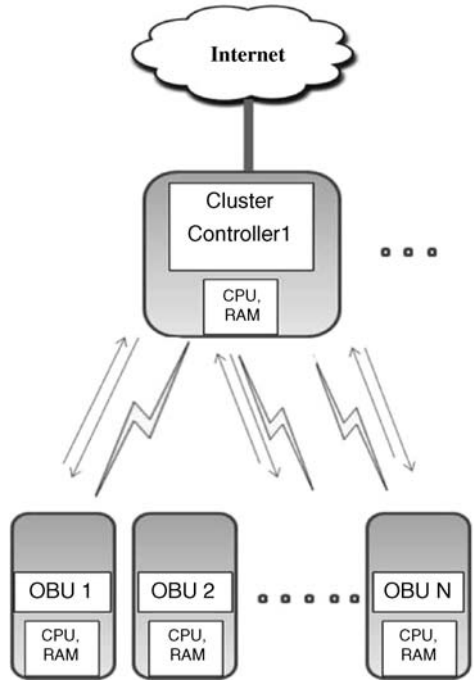

Figure 19.12 OBU load balancing.

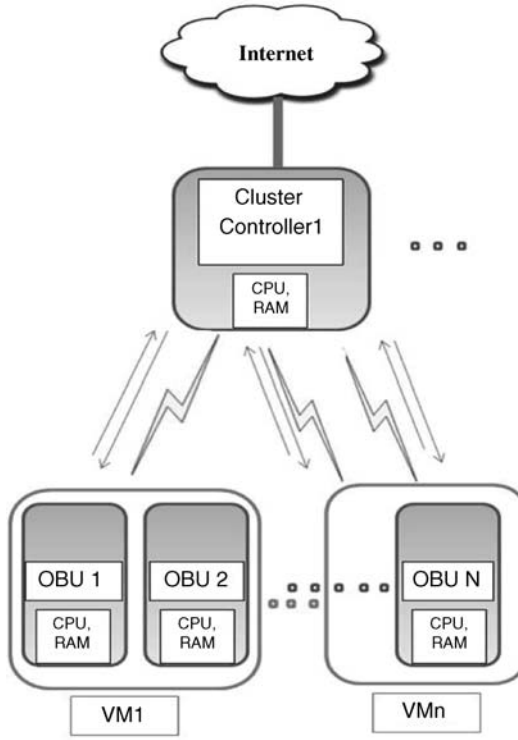

Figure 19.13 VM formation.

security overhead, would lead to a total initial transfer of 420 MB. Considering an 802.11a wireless communication channel, such an image would translate to an initial data transfer of 9 s, or 0.42 s when a 1-gigabit Ethernet channel is utilized. After this initial delay, a new note instance will be equipped with the same OS image running on the rest of the nodes associated with a particular VM image. Figure 19.14 presents this initial data exchange between the nodes involved. This approach allows a service to be run on multiple images and thus create the notion of a single large VM image.

19.13.2.2 Node Deregistration. When a vehicle leaves the cluster, the cluster controller will have to ensure that all client sessions are handled accordingly and that the service response times required for the VM affected are still met within acceptable delay limits. This process is called node deregistration, and it will be initiated when the node controller notifies the cluster controller that it must disjoin. The cluster controller will then initiate a timeout period during which it will wait for another vehicle to join the cluster. In case this period is exceeded and a new node has not joined, all neighboring cluster controllers will be contacted in order to request a replacement for the one deregistering. Based on the communication range of the requesting controller, the neighboring ones will determine whether they can provide a node. Figure 19.15

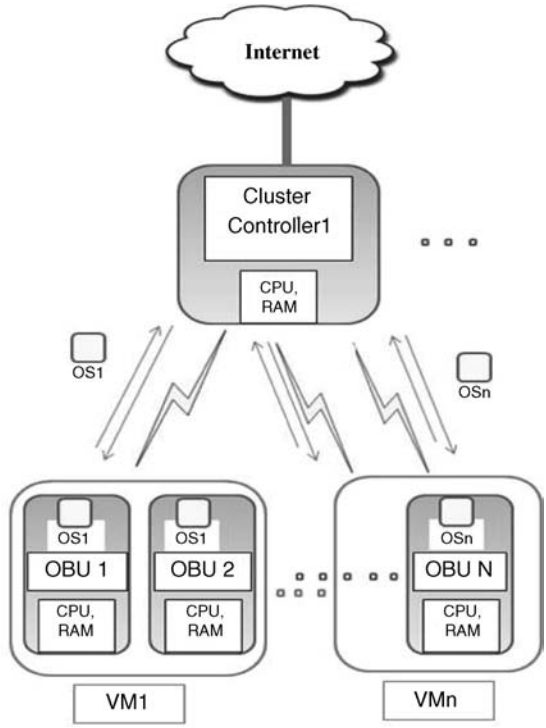

Figure 19.14 Node registration.

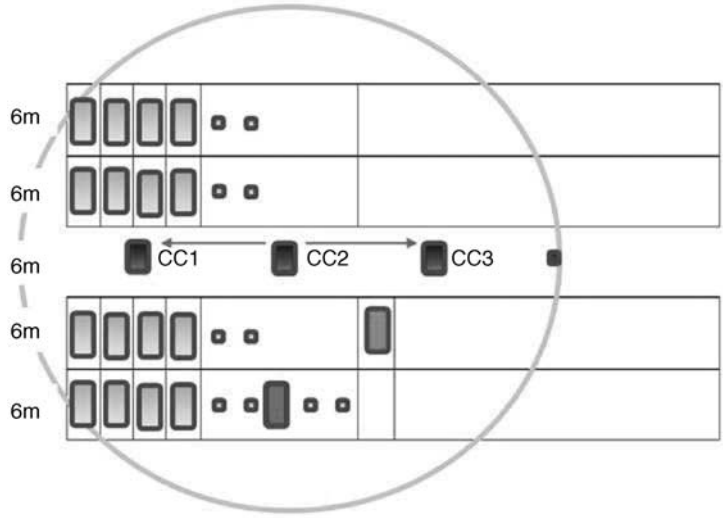

Figure 19.15 Illustrating node deregistration.

illustrates the case where a controller CC2 requests node replacements from CC1 and CC2, CC2 finds a node and allows the registration replacement. When a new vehicle joins the CC2 cluster, the "borrowed" node will be returned to the control of CC3.

19.14 A SIMULATION STUDY OF VC

In order to evaluate the proposed method of a Load Balanced Autonomous Vehicular System, we have designed an NS-3 simulation of the parking lot environment depicted in Figure 19.11. Table 19.1 presents the values used in the simulation. 150 meters section of a parking lot has been designed. This includes 200 parking spots, 6 m in length and 3 m in width. All vehicles are created with 2-m width and 4-m length dimensions, with a 2-m gap in between. All vehicles are static and the simulations does not include an investigation of the mobility aspect of the VC. Each vehicle has been equipped with a wireless communication device that implements an 802.11a wireless channel with data rate of 54 Mbps. Each run of the simulation is set to be 20 s.

19.14.1 Simulation Scenarios

The simulation will present a web server VM. As stated in reference 74, the average web page size in 2010 was 507 KB, and this will be the average http request this server will handle. The cluster controllers will handle incoming requests, relay them to node controllers associated with VMs, and then send the results back to the clients. During the simulation, the load on each VM and the number of node controllers inside a VM (OBU density) will be modified. Values for the OBU density will be 20, 40, and 100 OBUs per VM, and values for the server load will be 20, 100, and 200 requests per seconds (rps). Based on these values, the total number of scenarios would be 9.

19.14.2 Simulation Metrics

The scenarios presented in the previous subsection will provide an insight into the OBU density and the load a VM can handle. The metrics to be monitored are the

Table 19.1 Simulation Parameter Settings

Parameter	Value
Parking lot size	150 m
Parking spot length	6 m
Parking spot width	3 m
Vehicle length	4 m
Vehicle width	2 m
Vehicle gap	2 m
Communication channel	802.11a
Transmission rate	54Mbps
Simulation time	20 s

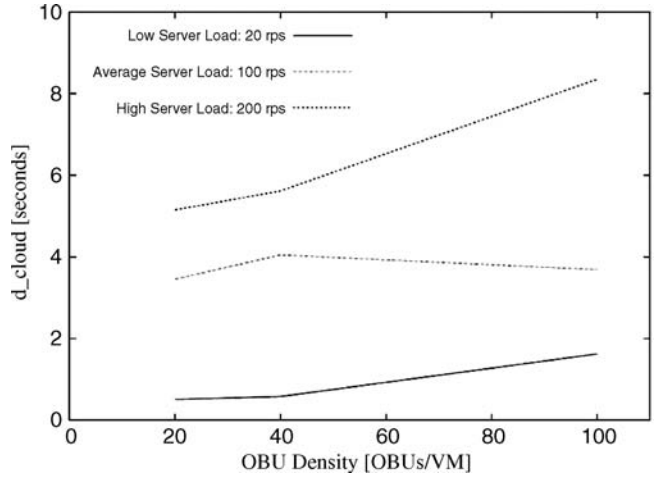

Figure 19.16 Cloud delay versus OBU density.

delay of the http reply imposed by the VC system: cloud delay (d_cloud). This value will be measured as the average value per session. A second metric to be monitored is retransmission rate: the average number of packet retransmissions for a single http session.

19.14.3 Simulation Results

Figure 19.16 illustrates the results of the cloud delay versus OBU density simulation scenarios. The three lines depict the d_cloud data for three different load values (20, 100, 200 rps). The results display that using an 802.11a channel, the minimum delay imposed by the VC is 0.5 s. It can be also observed that increasing the OBU density leads to a higher delay on the system. As a result, the proposed load-balanced VC must be designed with a high RSU density and thus a low OBU density. The second metrics of interest presented in this simulation is the retransmission rate compared to the OBU density Figure 19.17. As expected, the higher OBU densities lead to higher retransmission rates, since more units compete for access to the wireless channel and thus increase the number of collisions and retransmissions. An interesting result is that the retransmission rate for low server loads is the largest of all three load scenarios. That value later is superseded by the average server load simulations. An unexplained result is the fact that the high server load scenarios (200 rps) have the least retransmission rates. This observation is to be further analyzed.

19.15 FUTURE WORK

One main component not taken into consideration during this work is the effect of storage on the VC model. Figure 19.18 presents a proposed model for a storage

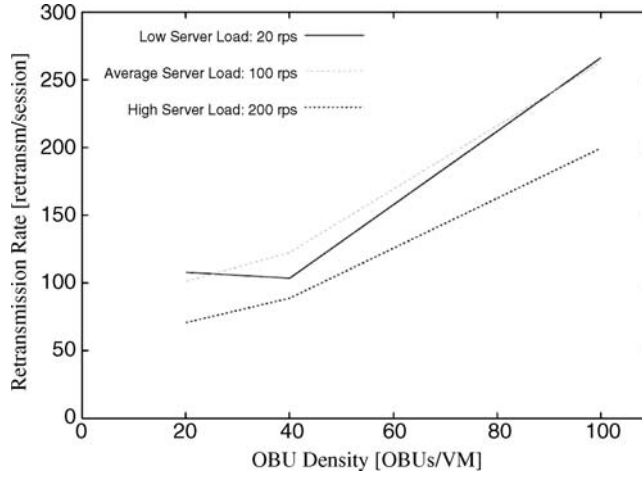

Figure 19.17 Retransmission versus OBU density.

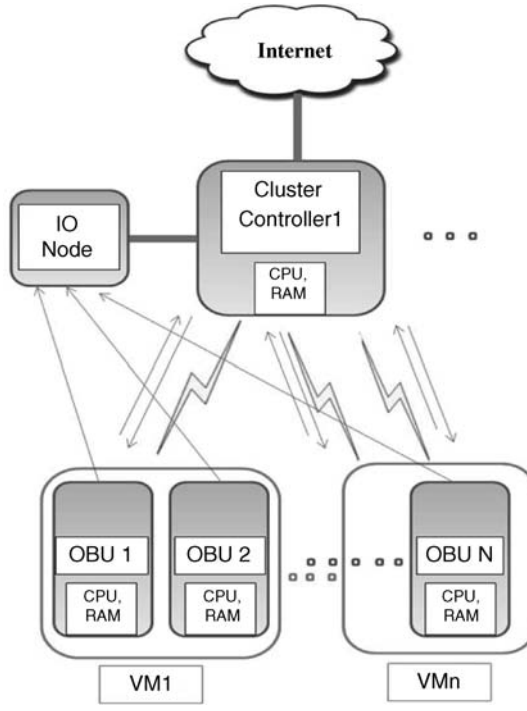

Figure 19.18 IO effect.

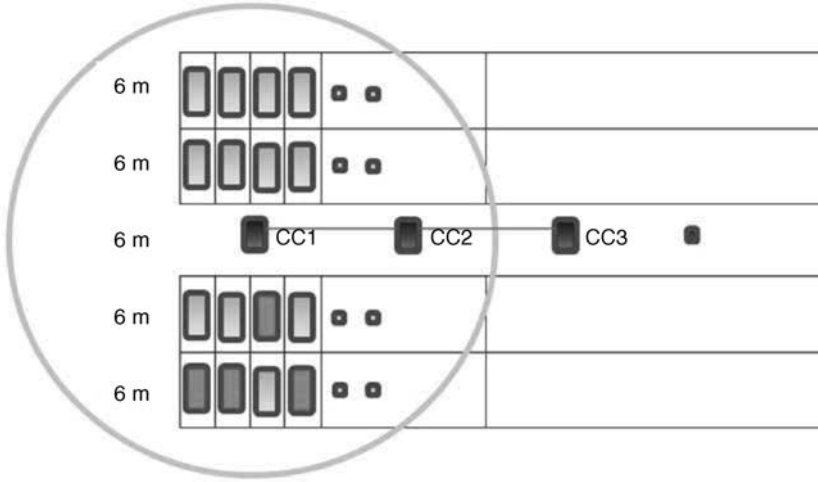

Figure 19.19 Illustrating dynamic spatial node reconfiguration.

solution. An additional IO Node is to be introduced to the cloud. The node will have a clustered file system that will allow the reading and writing of data by the multiple node and cluster controllers involved in a cloud. The effect of this node on the d_cloud and retransmission rates is to be evaluated.

A technique to decrease the delay and retransmission is proposed. The method entails selecting certain nodes within a cluster area to participate in the cloud communication. This technique is called dynamic spatial node reconfiguration (Figure 19.19) and is based on the fact that removal of the network transmission of specific nodes can improve the overall performance by reducing the channel competition and thus the number of unsuccessful transmissions. The model also includes power and data transmission rate control of all nodes in order to achieve a lower delay time. Future work will also include simulating the effect of multiple fading models on the VC performance.

19.16 WHERE TO FROM HERE?

In this chapter we have put forth a novel vision, namely that advances in vehicular networks, embedded devices, and cloud computing in conjunction with a tremendous amount of underutilized on-board resources in present-day vehicles are conducive to what we call vehicular clouds (VC). In such a VC, the underutilized vehicles resources such as computing power, Internet connectivity, and storage can be either shared between drivers or rented over the Internet to various customers, very much like the usual cloud resources [94–99].

We made the point that some of these resources can be harvested dynamically in support of mitigating traffic events. The typical scenario is that in the face of a traffic event the municipality that has the authority and the code but not the resources to run

the code on will enlist the help of the vehicles affected by the traffic events (i.e., stuck in traffic) to provide the computational resources on which the code can be run. We see the resulting symbiotic cooperation between the municipality and the traveling public as one of the most important contributions of the vehicular cloud concept.

We believe it is not too far-fetched to imagine, in the not-so-distant-future, a large-scale federation of VCs established ad hoc in support of mitigating a large-scale emergency. One of these large-scale emergencies could be a planned evacuation in the face of a potentially deadly hurricane or tsunami that is expected to make land-fall in a coastal region [100]. Yet another such emergency would be a natural or man-made disaster apt to destroy the existing infrastructure and to play havoc with cellular communications. In such a scenario, a federation of VCs could provide a short-term replacement for the infrastructure and also provide a decision-support system.

VANET networks are the future of the driving experience the way we know it today. Intervehicular communication would allow for information to be propagated with the speed of light and save lives on the roads. Each vehicle will be equipped with a computing device that will have CPU, memory and storage resource. When underutilized, those devices are the perfect sources for CC hosts. The nature of a VC would allow for a scalable implementation within a VANET environment. Both mobile and static situations would provide the computing and networking power for a successful "pay-per-go" solution. The limited hardware specification of embedded vehicular computers are the only restriction toward employing the already developed virtualization and clustering techniques. As a result, two solutions have been proposed: OBU Virtualization and OBU Load Balancing. The first proposal has been evaluated as inapplicable to an VC solution due to the limited network transmission rates in a wireless medium. The second method of Load Balancing incoming request has achieved delay and retransmission rates higher than expected, but within acceptable limits. Techniques to solve all VC problems have been proposed and evaluated as functional. Future optimization of the load balancing technique have been proposed and are to be analyzed [101]. A DSRC simulation of the technique should also be conducted in order to test the mobile VC models.

ACKNOWLEDGMENTS

This work was supported by NSF grants CNS-0721523 and CNS-0721586. The authors wish to thank several colleagues for contributing directly or indirectly to making this chapter possible. Here is the list of folks we acknowledge in alphabetical order: Mahmoud Abuelela, Mohamed Eltoweissy, Michael Fontaine, Ismail Khalil, Jin Wang, Michele Weigle, and Mohamed Younis.

REFERENCES

1. US Federal Communications Commission (FCC). Standard Specification for Telecommunications and Information Exchange Between Roadside and Vehicle Systems—5 GHz

Band Dedicated Short Range Communications (DSRC) Medium Access Control (MAC) and Physical Layer (PHY) Specifications, Washington, DC. September 2003.

2. M. Abuelela and S. Olariu. Content delivery in zero-infrastructure VANET. In *Vehicular Networks: From Theory to Practice*, S. Olariu and M. C. Weigle, Eds, Taylor and Francis, Boca Raton, FL, 2009, pp. 8.1–8.15.
3. J. Eriksson, H. Balakrishnan and S. Madden. Cabernet: Vehicular content delivery using WiFi. In *Proceedings 14th ACM International Conference on Mobile Computing and Networking* (MobiCom'2008), San Francisco, September 2008.
4. L. Le, A. Festag, R. Baldesari and W. Zhang. CAR-2-X Communications in Europe. In *Vehicular Networks: From Theory to Practice*, S. Olariu and M. C. Weigle, Eds., Taylor and Francis, Boca Raton, FL, 2009, pp. 8.1–8.32.
5. U. Lee, R. Cheung and M. Gerla. Emerging vehicular applications. In *Vehicular Networks: From Theory to Practice*, S. Olariu and M. C. Weigle, Eds., Taylor and Francis, Boca Raton, FL, 2009, pp. 6.1–6.30.
6. Tropos Networks, http://www.tropos.com/pdf/solutions/Parking-Final.pdf, 2010.
7. National Highway Traffic Safety Administration, Traffic Safety Facts, http://www-nrd.nhtsa.dot.gov, 2006.
8. S. Palmer. NHTSA's final ruling for automotive EDRs will revolutionize auto insurance. A draft, August 2006.
9. US Department of Transportation. National Transportation Statistics, 2008.
10. US Department of Transportation. Federal-Aid Highway Program Guidance on High Occupancy Vehicle (HOV) Lanes, http://ops.fhwa.dot.gov/freewaymgmt/hovguidance/index.htm, August 2008.
11. Virginia Department of Transportation. Commonwealth of Virginia's Strategic Highway Safety Plan, 2006-2010, http://virginiadot.org/info/resources/Strat_Hway_Safety_Plan_FREPT.pdf, 2006.
12. Sightline, http://www.sightline.org/research/energy/respubs/analysis-ghg-roads, 2009.
13. M. Fontaine. Traffic monitoring. In *Vehicular Networks: From Theory to Practice*, S. Olariu and M. C. Weigle, Eds, Taylor and Francis, Boca Raton, FL, 2009, pp. 1.1–1.28.
14. US Department of Transportation. Catastrophic Hurricane Evacuation Plan Evaluation: A Report to Congress, http://www.fhwa.dot.gov/reports/hurricanevacuation/, June 2006.
15. National Highway Traffic Safety Administration, Traffic Safety Facts—preliminary 2009 report, http://www-nrd.nhtsa.dot.gov/Pubs/811255.pdf, March 2010.
16. T. ElBatt, S. Goel, G. Holland, H. Krishnan, and J. Parikhan. Cooperative collision warning using dedicated short range wireless communications. In *Proceedings 3rd ACM International Workshop on Vehicular Ad Hoc Networks* (VANET'2006), May 2006.
17. J. Rybicki, B. Scheuermann, M. Koegel, and M. Mauve. PeerTIS: A peer-to-peer traffic information system. In *Proceedings of the 6th ACM International Workshop on Vehicular Ad Hoc Networks*, (VANET'09), Beijing, China, September 2009.
18. J. A. Misener, S. Dickey, J. VanderWerf and R. Sengupta. Vehicle-infrastructure cooperation. In *Vehicular Networks: From Theory to Practice*, S. Olariu and M. C. Weigle, Eds., Taylor and Francis, CRC Press, Boca Raton, FL, 2009, pp. 3.1–3.35.
19. R. Sengupta, S. Rezaei, S. E. Shlavoder, D. Cody, S. Dickey, and H. Krishnan. Cooperative collision warning systems: Concept definition and experimental implementation, California PATH Technical Report UCB-ITS-PRR-2006-6, May 2006.

20. R. P. Roess, E. S. Prassas, and W. R. McShane. *Traffic Engineering*, 4th Edition. Pearson Prentice Hall, Upper saddle River, NJ, 2010.
21. I. Sreedevi and J. Black, Loop Detectors, California Center for Innovative Transportation, http://www.calccit.org/itsdecision/serv_and_tech/Traffic_Surveillance/road-based/in-road/loop_report.html, 2001.
22. P. Varaiya, X.-Y. Lu, and R. Horowitz. Deliver a Set of Tools for Resolving Bad Inductive Loops and Correcting Bad Data, http://path.berkeley.edu/∼xylu/TO6327/TO6327_SEMP.pdf, October 2006.
23. University of Virginia Center for Transportation Studies, Virginia Transportation Research Council, Probe-Based Traffic Monitoring State-of-the-Practice Report, November 2005.
24. A. Aijaz, B. Bochow, F. Doetzer, A. Festag, M. Gerlach, R. Kroh and T. Leinmueller. Attacks on inter-vehicle communication systems: An analysis, In *Proceedings of International Workshop on Intelligent Transportation* (WIT'2006), Hamburg, Germany, March 2006.
25. C. Lochert, B. Scheuermann, M. Caliskan and M. Mauve. The feasibility of information dissemination in vehicular ad hoc networks. In *Proceedings of the 4th Annual Conference on Wireless On-demand Network Systems and Services*, (WONS'07), January 2007, pp. 92–99.
26. C. Lochert, B. Scheuermann, C. Wewetzer, A. Luebke and M. Mauve. Data aggregation and roadside unit placement for a VANET traffic information system. In *Proceedings of 5th ACM International Workshop on Vehicular Ad Hoc Networks* (VANET'08), September 2008.
27. G. Yan, S. Olariu, and M. C. Weigle. Providing VANET security through active position detection, *Computer Communications* **31**(12):2883–2897, 2008.
28. G. Yan, S. Olariu, and M. Weigle, Providing location security in vehicular ad hoc networks, *IEEE Wireless Communications* **16**(6):48–55, 2009.
29. Y. Yang and R. Bagrodia. Evaluation of VANET-based advanced intelligent transportation systems. *Proceedings of the 6th ACM International Workshop on Vehicular Ad Hoc Networks* (VANET'09), Beijing, China, September 2009.
30. J. Anda, J. LeBrun, D. Ghosal, C.-N. Chuah and M. Zhang. VGrid: Vehicular ad hoc networking and computing grid for intelligent traffic control. In *Proceedings of IEEE Vehicular Technology Conference*—Spring, May 2005, pp. 2905–2909.
31. K. Czajkowski, S. Fitzgerald, I. Foster and C. Kesselman. Grid information services for distributed resource sharing. In *Proceedings of 10th IEEE International Symposium on High Performance Distributed Computing*, New York, 2001, pp. 181–184.
32. National Institute of Standards and Technology, NIST Definition of Cloud Computing, http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc, October 2009.
33. J. Foley. Private Clouds Take Shape, *Information Week*, August 9, 2008.
34. S. Hodgson, What Is Cloud Computing? http://www.winextra.com/2008/05/02/what-is-cloud-computing.pdf, May 2, 2008.
35. J. N. Hoover and R. Martin. Demystifying the cloud. *InformationWeek Research & Reports* **June**:30–37, 2008.
36. W. Kim. Cloud Computing: Today and Tomorrow, *Journal of Object Technology* **8**(1): 65–72, January–February 2009. http://www.jot.fm/issues/issue_2009_01/column4/.

37. Woodford, Inc., Cloud Computing Explained, http://www.explainthatstuff.com/cloud-computing-introduction.html, Feb. 5 2010.
38. Sun Microsystems. EUCALYPTUS: Open Source Cloud Infrastructure, The Skies Are Opening, http://blogs.sun.com/WebScale/entry/eucalyptus_skies_are_opening, Nov. 10 2008.
39. M. Abuelela and S. Olariu. Taking VANET to the clouds. In *Proceedings of ACM MoMM*, Paris, France, November 2010.
40. S. Arif, S. Olariu, J. Wang, G. Yan, W. Yang, and I. Khalil. Datacenter at the airport: Reasoning About Time-Dependent Parking Lot Occupancy. *IEEE Transactions on Parallel and Distributed Systems* **23**(11):2067–2080, 2012.
41. M. Eltoweissy, S. Olariu and M. Younis. Towards autonomous vehicular clouds. In *Proceedings AdHocNets*, Victoria, BC, Canada, August 2010.
42. S. Olariu, I. Khalil, and M. Abuelela. Taking VANET to the Clouds, *International Journal of Pervasive Computing and Communications* **7**(1):7–21, 2011.
43. S. Olariu, M. Eltoweissy, and M. Younis. Towards autonomous vehicular clouds, *ICST Transactions on Mobile Communications and Computing* **11**(7–9):1–11, 2011.
44. P. Edara and C. McGhee. An Operational Analysis of the Hampton Roads Hurricane Evacuation Traffic Control Plan—Phase 2, Virginia Transportation Research Council, 2008.
45. T. Litman. Lessons from Katrina and Rita: What major disasters can teach transportation planners. *ASCE Journal of Transportation Engineering*. **132**(1):11–18, 2006.
46. P. M. Murray-Tuite and H. S. Mahmassani. Transportation network evacuation planning with household activity interactions. *Transportation Research Record: Journal of Transportation Research Board*, **1894**:150–159, 2004.
47. www.citrix.com. Virtualization, Networking and Cloud Computing, 2009.
48. www.vmware.com, VMware Virtualization Software for Desktops, Servers & Virtual Machines for Virtual and Public Clouds, 2009.
49. VMware Inc. Resource Management with VMware DRS, November 2007.
50. VMware Inc. Understanding Full Virtualization, Paravirtualization, and Hardware Assist, September 11, 2007.
51. VMware Inc. A Performance Comparison of Hypervisors, November 2007.
52. Scarborough Research/Arbitron Inc. Teen mall shopping insights. A white paper, June 2009.
53. J. Skolnik, R. Chami, and M. Walker. Planned Special Events—Economic Role and Congestion Effects, Technical Report FHWA-HOP-08-022, Federal Highway Administration, U.S. Department of Transportation, Washington, D.C., 2008.
54. US Department of Transportation, Intelligent Transportation Systems for Planned Special Events: A Cross-Cutting Study, Technical Report FHWA-JPO-08-056, Federal Highway Administration, Washington, D.C., 2008.
55. Trafficware Ltd. Synchro 7 User Manual, 2006.
56. US Department of Transportation, Federal-Aid Highway Program Guidance on High Occupancy Vehicle (HOV) Lanes, http://ops.fhwa.dot.gov/freewaymgmt/hovguidance/index.htm, August 2008.
57. N. Wilson-Goure and A. Vann Easton, Case Studies: Assessment of the State of the Practice and State of the Art in Evacuation Transportation Management, Technical Report FHWA-HOP-08-014, Federal Highway Administration, Washington, D.C., 2006.

58. M. K. Lindell and C. S. Prater. Critical behavioral assumptions in evacuation time estimate analysis for private vehicles: Examples from hurricane research and planning. *Journal of Urban Planning and Development*. **133**(1):18–29, 2007.
59. Automated Parking Management System at New Hyderabad International Airport, http://www.inrnews.com/realestateproperty/india/hyderabad/automated_parking_management_s.html, 2009.
60. G. Yan, W. Yang, D. B. Rawat and S. Olariu. SmartParking: A secure and intelligent parking system. In *IEEE Intelligent Transportation Systems Magazine* **3**(1):18–30, 2011.
61. M. Eltoweissy, S. Olariu, and M. Younis, ANSWER: Autonomous Networked Sensor System, *Journal of Parallel and Distributed Computing* **67**(1):111–124, 2007.
62. A. Friedman and D. West. Privacy and security in cloud computing. *The Centre for Technology Innovation: Issues in Technology Innovation* **3**:1–11, 2010.
63. S. Olariu and M. C. Weigle, Eds. *Vehicular Networks: From Theory to Practice*, CRC Press/Taylor & Francis, Boca Raton, FL, 2009.
64. J. A. Blackley, J. Peltier, and T. R. Peltier. *Information Security Fundamentals*, Auerbach Publications, 2004, 14(1), http://www.amazon.co.uk/Information-Security-Fundamentals-John-Blackley.
65. N. Santos, K. P. Gummadi, and R. Rodrigues. Towards trusted cloud computing. In *Proceedings of HotCloud*, June 2009.
66. T. Garfinkel, B. Pfaff, J. Chow, M. Rosenblum, and D. B. Terra. Virtual machine-based platform for trusted computing. In *Proceedings of ACM Symposium on Operating Systems Principles SOSP*, 2003.
67. S. Berger, R. Caceres, K. A. Goldman, R. Perez, R. Sailer, and L. van Doorn. vtpm: virtualizing the trusted platform module. In *Proceedings of the 15th Conference on USENIX Security Symposium*, Vol. 15. USENIX Association, Berkeley, CA, 2006.
68. D. G. Murray, G. Milos, and S. Hand. Improving xen security through disaggregation. In *Proceedings of the Fourth ACM SIGPLAN/SIGOPS International Conference on Virtual Execution Environments*, Ser. VEE '08, ACM, New York, 2008, pp. 151–160.
69. F. J. Krautheim, Private virtual infrastructure for cloud computing. In *Proceedings of the IEEE Conference on Hot Topics in Cloud Computing*, 2009, pp. 1–5.
70. M. Jensen, J. Schwenk, N. Gruschka, and L. L. Iacono. On technical security issues in cloud computing. In *Proceedings of the IEEE International Conference on Cloud Computing*, 2009, pp. 109–116.
71. C. Wang, Q. Wang, K. Ren, and W. Lou. Privacy-preserving public auditing for data storage security in cloud computing, *Proceedings of the IEEE International Conference on Computer Communications*, (INFOCOM'10), San Diego, CA, 2010, pp. 1–9.
72. Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou. Enabling public verifiability and data dynamics for storage security in cloud computing. In *Proceedings of the 14th European conference on Research in Computer Security*, (ESORICS'09), Springer-Verlag, Berlin, 2009, pp. 355–370.
73. T. Ristenpart, E. Tromer, H. Shacham, and S. Savage. Hey, you, get off of my cloud: Exploring information leakage in third-party compute clouds. *Proceedings of the 16th ACM Conference on Computer and Communications Security* (CCS '09), 2009, pp. 199–212.
74. J. Y. Choi, P. Golle, and M. Jakobsson. Tamper-evident digital signatures: Protecting certification authorities against malware. In *Proceedings IEEE International Symposium on Dependable, Autonomic and Secure Computing (DASC'06)*, 2006, pp. 37–44.

75. J.-P. Hubaux, S. Capkun, and J. Luo. The security and privacy of smart vehicles. *IEEE Security and Privacy Magazine* **2**(3):49–55, 2004.
76. M. Raya, P. Papadimitratos, and J.-P. Hubaux. Securing vehicular communications. *IEEE Wireless Communications Magazine* 8–15, 2006.
77. J. Sun, C. Zhang, Y. Zhang, and Y. M. Fang, An identity-based security system for user privacy in vehicular ad hoc networks, *IEEE Transactions on Parallel Distributed System* **21**:1227–1239, 2010.
78. K. P. Laberteaux, J. J. Haas, and Y.-C. Hu. Security certificate revocation list distribution for VANET. In *Proceedings of the Fifth ACM International Workshop on Vehicular Internetworking*, (VANET '08), 2008, pp. 88–89.
79. D. E. Denning and P. F. MacDoran. Location-based authentication: Grounding cyberspace for better security. *Computer Fraud & Security* **1996**(2):12–16, 1996.
80. L. Scott and D. E. Denning. Location based encryption technique and some of its applications. In *Proceedings of the Institute of Navigation National Technical Meeting 2003*, Anaheim, CA, January 22–24, 2003, pp. 734–740.
81. G. Yan and S. Olariu. An efficient geographic location-based security mechanism for vehicular ad hoc networks. In *Proceedings of the 2009 IEEE International Symposium on Trust, Security and Privacy for Pervasive Applications (TSP-09)*, Macau SAR, China, October 12–14, 2009.
82. G. Yan and S. Olariu, A probabilistic analysis of link duration in vehicular ad hoc networks. *IEEE Transactions on Intelligent Transportation Systems* **12**(3):1–10, 2011.
83. H. Xie, L. Kulik, and E. Tanin, Privacy-aware traffic monitoring. *IEEE Transactions on Intelligent Transportation Systems* **11**(1):61–70, 2010.
84. D. Huang, S. Misra, G. Xue, and M. Verma. PACP: An efficient pseudonymous authentication based conditional privacy protocol for vanets, *IEEE Transactions on Intelligent Transportations* **3**(12): 736–746, 2011.
85. Microsoft Corporation. The Stride Threat Model, http://msdn.microsoft.com, 2002.
86. M. Raya and J. P. Hubaux. Securing vehicular ad hoc networks. *Journal of Computer Security* **15**(1):39–68, 2007.
87. Federal Financial Institutions Examination Council. Authentication in an Internet Banking Environment, 2009, http://www.ffiec.gov/pdf/authentication_guidance.pdf
88. T. ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms, *IEEE Transactions on Information Theory* **31**(4):469–472, 1985.
89. C. Valli and A. Woodward. The 2008 Australian study of remnant data contained on 2nd hand hard disks: The saga continues, 2008.
90. M. Raya, D. Jungels, P. Papadimitratos, I. Aad, and J. P. Hubaux. Certificate revocation in vehicular networks. Technical Report, 2006.
91. D. Nurmi, R. Wolski, C. Grzegorczyk, G. Obertelli, S. Somana, L. Youseff, and D. Zagorodnov. The EUCALYPTUS Open-Source Cloud-Computing System, *Proceedings of IEEE/ACM International Symposium on Cluster Computing and the Grid (CCGRID)*, May 2009, pp. 124–131.
92. J. Ott and D. Kutscher. Drive-thru Internet: IEEE 802.11b for Automobile Users. In *Proceedings of the IEEE INFOCOM*, 2004.
93. Cisco Systems, Inc. Understanding CSM Load Balancing Algorithms, November 30 2005.

94. J. Ott and D. Kutscher. A disconnection-tolerant transport for drive-thru Internet environments. *Proc. IEEE INFOCOM*, 2005.

95. J. Rybicki, B. Scheuermann, W. Kiess, C. Lochert, P. Fallahi, and M. Mauve. Peers on wheels: A road to new traffic information systems. In *Proceedings of the 13th Annual ACM International Conference on Mobile Computing and Networking* (MobiCom'07), Montreal, September 2007.

96. SIRIT-Technologies, DSRC Technology and the DSRC Industry Consortium Prototype Team, White Paper, http://www.itsdocs.fhwa.dot.gov/research_docs/pdf/45DSRC-whitepaper.pdf, 2005.

97. W.-L. Tan, W.-C. Lau and O.-C. Yue. Modeling resource sharing for a road-side access point supporting drive-thru Internet. In *Proceedings of the 6th ACM International Workshop on Vehicular Ad Hoc Networks*, (VANET'09), Beijing, China, September 2009.

98. US Department of Transporation. Research and Innovative Technology Association, National Transportation Statistics, http://www.bts.gov/publications/national_transportation_statistics/, 2010.

99. Q. Xu, T. Mak, J. Ko and R. Sengupta, Vehicle-to-vehicle safety messaging in DSRC. In *Proceedings of the 1st ACM International Workshop on Vehicular Ad Hoc Networks* (VANET'2004), October 2004.

100. D. Feldstein and M. Stiles. Too many people and no way out. *The Houston Chronicle*, September 25, 2005.

101. WebsiteOptimization.com, http://www.websiteoptimization.com/speed/tweak/average-web-page/, Jul. 31 2010.