Connected Parking and Automated Valet Parking

10

This chapter discusses one of the most relevant and straightforward application of connected cars—connected parking. Everybody who is driving a car has had some experience with the difficulty to find a parking space and to park the car in narrow lots. Fortunately, technology is available to help, and it will potentially have a major impact on traffic, parking accidents and space utilization in cities. After a brief discussion of parking from a business perspective in Sect. 10.1, analyzing the main challenges, the chapter discusses the opportunities for connected parking in Sect. 10.2. A multitude of new apps provides information, often in real-time, about available parking spaces; manages the booking; often allows for cashless billing; and can be integrated with OEM's connectivity services. This chapter gives an overview of major players and discusses the core features and services of their solution. Section 10.3 presents parking assistance systems. The most sophisticated—as of today—automates the complete parking process; however, the driver still has to be in the car and has to oversee the process. The next step, automated valet parking (AVP), is discussed in Sect. 10.4. AVP systems turn the vehicle into a robot car that automatically finds parking space and maneuvers the car into a free slot. The first commercial systems will soon be available in high-end cars, and also will be deployed for carsharing. Sections 10.5 and 10.6 deal with the cybersecurity impact of connected parking and automated valet parking, analyzing the major cyber threats and look at potential solutions for increasing the cybersecurity, like intrusion detection and prevention (see also Chap. 6). Such systems are in place to protect large-scale IT infrastructure and recently have been applied to the cybersecurity of vehicles, which is discussed more in detail in Chap. 6. Section 10.7 finally wraps up with a conclusion and recommended further readings. Section 10.8 contains a comprehensive set of questions on connected parking and automated valet parking and the final section includes references and further readings.

D. P. F. Möller, R. E. Haas, *Guide to Automotive Connectivity and Cybersecurity*,
Computer Communications and Networks,
https://doi.org/10.1007/978-3-319-73512-2_10

10.1 Parking

The parking industry is comprised of many players and stakeholders (URL1 2017). Parking space at airports, railway stations, shopping malls, and public park-and-ride lots accounts for large real estate demand in urban areas. People spend a lot of time searching for parking space. Volkswagen (VW) estimates that up to 30% of the inner-city traffic is due to the search for parking space (Jungwirth 2016; Gerster 2016; Rees 2016). One can differentiate on-street parking, often managed by cities or freely available and off-street parking in special marked places, like huge parking lots, multistorey buildings, and park-and-ride facilities. These off-street parking areas are typically managed by large parking operators like Apcoa (URL21 2017). They lease the space, provide the necessary infrastructure, and manage the billing. The biggest car park operators in Europe are Apcoa, Germany, with a 10% market share; Q-Park, Netherlands (URL22 2017); and Contipark, Belgium (URL23 2017), as shown in Fig. 10.1.

The car park business and the market are characterized by the following:

- Market is extremely fragmented, especially in Europe.
- Car park operators typically do not own the properties themselves but operate and maintain them.
- There are also many regional small- and mid-sized companies, as well as cities that manage the car parks and park houses themselves.
- Market is very competitive, operators are struggling with low margins, and some are even under loss (Dierig 2012). Because of this, park operators are reluctant to invest which often leads to old IT and outdated infrastructure.
- Car park operators are looking for new services to boost their revenues and profits, for example, cleaning the cars while being parked.

Fig. 10.1 The European market for parking is fractured - some of the leading parking operators

- New parking operators like Park One (URL20 2017) are focusing on services like valet parking.
- Cities cooperate with new players like Cleverciti, Parkpocket, and others (URL19 2017; URL3 2017), to provide real-time data about availability of parking space, both on-street and off-street, cutting down on search time and inner-city traffic.

10.2 Connected Parking

Finding parking space in a crowded city is a problem, which goes far beyond wasting time and it is one of the major reasons for the boom of carhailing and ridesharing providers. The main issues and challenges can be summarized as follows:

- Up to 30% of inner-city traffic is due to the search for parking space (Gerster 2016).
- Parking in cities can be very costly.
- Often, it is not clear where to find parking space.
- Looking out for parking while driving, especially, if one is alone in the car, is one of the main reasons for traffic accidents in the cities.
- Up to 40% of all accidents are related to parking (Gerster 2016).
- Theft and damage to the car in a parking lot is a major problem.
- Finding the car in a big parking lot is not easy.

The smartphone and the ideas of the shared economy (Laudon et al. 2010) also had a major impact on the way people park today.

Many start-ups have come up offering apps for connected parking (URL2 2017; URL8 2017; URL9 2017; URL10 2017; URL11 2017; URL15 2017):

- Parkopedia
- JustPark
- SpotHero
- ParkWhiz
- ParkingPanda
- BestParking

For on-street parking some of the popular apps are (URL12 2017; URL13 2017):

- Parker
- ParkMe
- ParkNow

The main idea is to provide information about available parking space, thereby, minimizing unnecessary traffic to search for a parking lot. Many apps use a community-/crowd-based mechanism to notify other drivers about available parking space. A particularly valuable information is the price of parking space which can vary

widely. Booking and reservation of a parking spot is another helpful service, often with attractive offers. Finally, the billing can be handled automatically, avoiding all sorts of hassles when trying to pay at the ticket machine because of not enough cash, no change, loss of park ticket, credit card not accepted, machine is down, and other possibilities. Also, electronic tracking of the invoices for parking is a nice feature that people appreciate in travel booking systems like Concur.

Big benefits can be achieved if the information is given in real-time. Some companies, e.g., the German start-up Ampido, are offering an Airbnb-type business model where one can advertise private car parks and rent them out via the platform (URL16 2017).

Parkopedia has undergone an interesting development. Started first as a kind of encyclopedia for parking space, aggregating available information about parking lots in various cities, it has added more and more features to the system, like real-time availability of parking, reserving space, billing, and predictive parking.

It is clear that the value of a parking platform grows with the reach (cities and regions), the number of parking lots, and the size of the user community. Predictive parking, the deployment of big data and machine learning to estimate free parking, is a promising area where parking apps can differentiate themselves from each other (URL18 2017). The best results can be achieved if data from all available sources is being combined, e.g.:

- Real-time traffic information
- Real-time data from parking operators
- Community-based information fed in through special apps or automatically via sensors (e.g., see Bosch IoT cloud)
- Statistical models taking into account time, date, special events, vacation time, etc.

Table 10.1 summarizes the core features of different parking solutions. Automotive OEMs have partnered up with connected parking apps to provide solutions for their car fleet, e.g., Daimler works with GottaPark (URL14 2017) and BMW integrates the services of Parkopedia (URL2 2017) into their connected drive infotainment system. Navigation and map providers, e.g., Tomtom (URL7 2017), also work with companies like Parkopedia to integrate parking value added services in their maps.

In Fig. 10.2 a different classification is shown based on the criterias on-street versus off-street and static versus dynamic real-time status of parking occupancy.

Real-time information about parking space can be gathered in various ways:

- Off-street: The parking operator can keep track and feed the information to a server.
- Specific sensors, embedded in the parking lot, can track, if a space is occupied or not. This can work both on-street and off-street, e.g., see projects by Siemens (URL31 2017), Bosch, ParkHere (URL29 2017).

Table 10.1 Features of parking apps compare (Chandrasekar et al. 2013; URL34 2017)

Parking app provider	Real-time parking and navigation	Parking reservation	Parking payment	On-street parking management	Region
Parkopedia	Yes	Yes	Yes	Yes	EU/US/APAC
ParkatmyHouse	Yes	Yes	Yes	No	EU/US
JustPark		Yes	Yes		EU
ParkNow	No	No	Yes		US
GottaPark	Yes	Yes	Yes	No	US
ParkingPanda	No	Yes	Yes	No	US
Streetline	Yes	Yes	Yes	Yes	EU/US

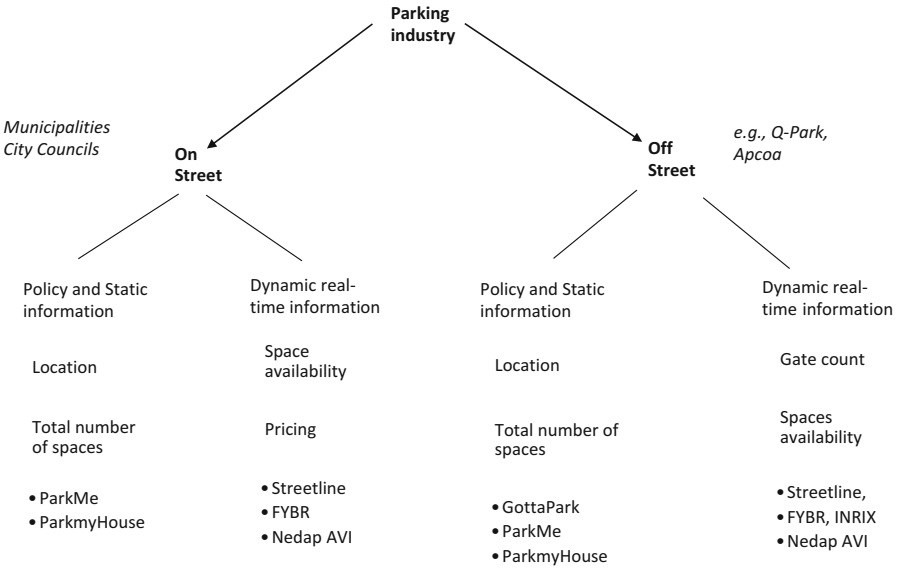

Fig. 10.2 Classification of parking apps/connected parking (Chandrasekar et al. 2013; URL34 2017)

- Car can gather information about free parking space when driving by using the in-built ultrasound sensors or cameras.
- Car can measure the dimension of free parking space.
- A car driver can explicitly notify others with a smartphone app about parking space availability.
- Movement of the car can be tracked automatically and can be used to predict if a parking space will be available.

Several parking operators like Apcoa are experimenting with a touchless access to the park house, e.g., based on an embedded RFID chip which is used for authentication and automatic payment. The potential of connected parking has attracted various large companies like SAP, Cisco, and others (URL1 2014; URL1 2016). The IAA 2015 provided a platform for several interesting start-ups that are now collaborating with some of the large players (URL3 2017; URL9 2015).

The San Francisco based company Streetline (URL4 2017) has a full service offering for cities, parking space operators, and car owners. It includes community-based real-time parking information, map integration of free parking spaces, billing, software systems and dashboards for off-street parking for cities and parking operators, as well. The analytics platform Parksight helps to optimize throughput, efficiency, and pricing decisions.

Another major player of parking solutions in the US is INRIX (URL5 2017). In 2014, Porsche acquired a 10% stake. The company offers community-based parking through its cloud platform, real-time parking information and solutions for parking operators and cities as well. Other services include real-time traffic information, state-wide traffic analytics, traffic collisions, parking data and analytics, connected car services, as well as traffic count and population movement insights. INRIX works with automakers and government agencies to understand how people and commerce move across the world's transportation network (URL31 2017).

In Fig. 10.3 the concept of community-based parking is explained (Nicodemus and Auracher 2015; URL25 2017; URL26 2017). If a car passes by an empty parking space on the side street, it will automatically scan the dimension with the in-built ultrasound and/or radar sensors. This can be done up to a speed of 50 km/h, i.e., within the speed limits of city traffic. The sensors can not only detect if a parking space is available but also how big the area is, thereby, providing information about

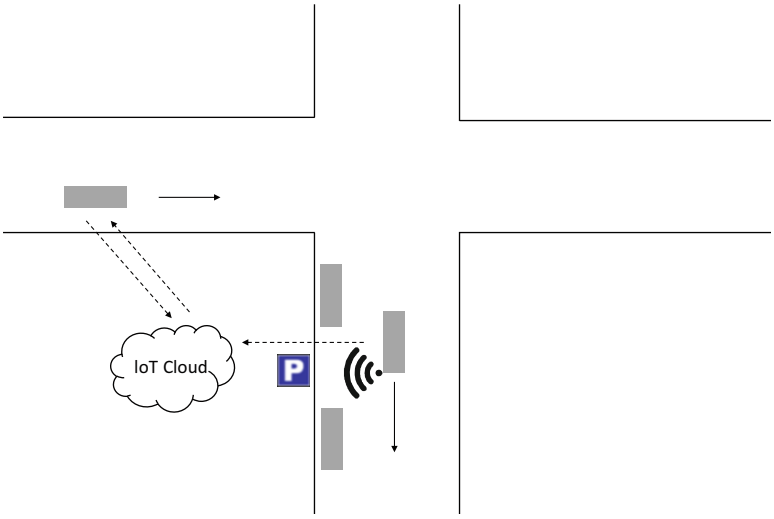

Fig. 10.3 Principle of Community-based parking (URL24 2017; URL26 2017; URL27 2017)

which type of cars could fit and which will not fit into the space. This information is gathered automatically and fed into the Bosch IoT cloud (URL27 2017). Here, the information is consolidated and made readily available to other cars which have subscribed to the cloud-based parking service.

In Fig. 10.3 the driver of the car on the left searches for parking space. The free parking space in the side street is not visible, but the information about a suitable parking lot which is currently free is available from the IoT cloud and shown on the map. The driver can decide to take it and pull into the parking space. If this happens, the system will automatically notify all other user that the parking space is now occupied.

The digital transformation of the parking industry leads to many new partnerships between OEMs, first tiers, start-ups, fleet managers, ride-hailing companies, etc. and has sparked interesting new business models. Figure 10.4 summarizes the different aspects of connected parking in a mind map (Nicodemus and Auracher 2015; Gebhardt 2016; URL24 2017). Frost and Sullivan have analyzed the parking industry and identified a point of conversion of partnerships and alliances as shown in Fig. 10.5 (Chandrasekar et al. 2013; URL35 2017).

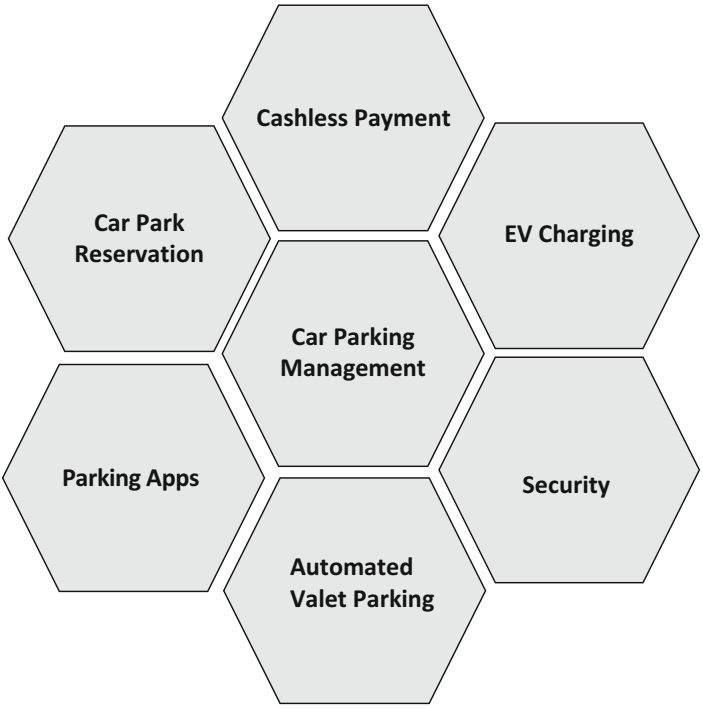

Fig. 10.4 Aspects of connected parking and the parking ecosystem (see also Nicodemus and Auracher 2015)

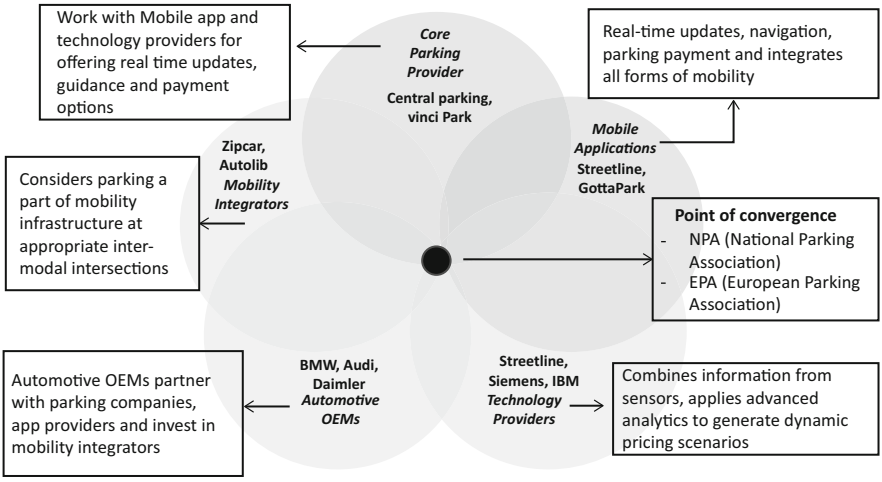

Fig. 10.5 Parking eco system (Chandrasekar et al. 2013)

10.3 Parking Assistance

Parking a car in a narrow parking slot can be challenging and is one of the main reasons for damages and repair work. Parking assistance systems can help. They are available for a couple of years now and especially popular in midrange to premium cars.

One can differentiate between different levels of functionality and complexity. The first and most simple system just alerts the driver of an obstacle via ultrasound sensors. A beep and/or visual signal is given, if the car comes too close to an obstacle in the rear, the front, or the side wall. These systems are particularly helpful in park houses with narrow parking lots. Rear cameras, which are mandatory in the USA since 2016, give additional overview and are helpful in combination with the ultrasound warning system.

The next level of parking assistance provides lateral control of the drive path by steering the car. The right sequence and pattern of steering maneuvers is often difficult. It can, however, be calculated precisely, and a computational algorithm can guide the car in an optimal way. These systems were first introduced in the early 1980s and are now widely available even in compact cars. Steering assistance requires the driver to constantly control the gas pedal and the breaking. The next level also relieves the driver from the longitudinal maneuvering. Steering and backing-off maneuvers are done automatically. However, the driver can apply breaks and overpower the parking assistance systems at any time.

Another level of automation is reached when the driver does not sit in the car anymore but oversees the park maneuver on his or her mobile phone.

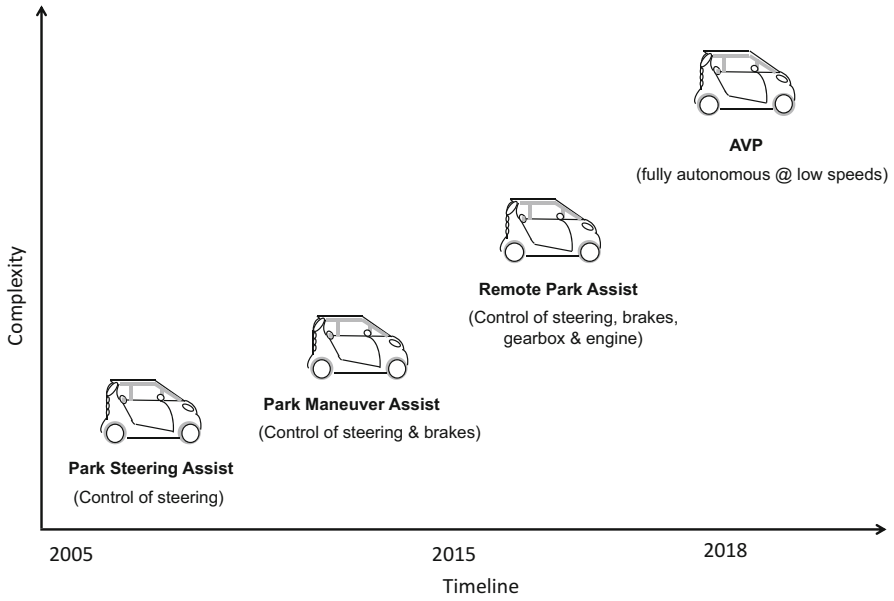

Fig. 10.6 Steps towards fully automated valet parking (see Nicodemus and Auracher 2015)

BMW and Mercedes offer systems for remote parking (Werle 2015). Mercedes uses the smartphone; BMW has developed a special key with an integrated display. As it is still not allowed to let the car drive completely alone, the driver has to oversee this process by constantly pressing a button. Various first-tier suppliers provide the technology, among them Bosch, Conti, Valeo, and ZF/TRW.

The highest level of automation is reached, if the driver only has to initiate the parking process, while the car finds the parking place, drives toward the slot, and maneuvers into the parking space without any further intervention and completely automatically. The concept is called automated valet parking (AVP). This chapter explores it in more detail in the next section. BMW demonstrated a remote parking assistance with AVP capabilities at the CES 2015 in Las Vegas (URL7 2015).

Figure 10.6 shows the evolution of automated valet parking driven by a combination of different sensor systems like ultrasound, radar and cameras.

10.4 Automated Valet Parking

Automated valet parking service (AVP) enables a vehicle to drive and park without any human interaction (Min and Choi 2013). This is most likely one of the first examples of fully autonomous driving being commercialized.

Bosch has introduced an automated valet parking functionality which combines both in-vehicle sensors (ultrasound sensors) and infrastructure-based technology (Gebhardt 2016; URL24 2017; URL25 2017).

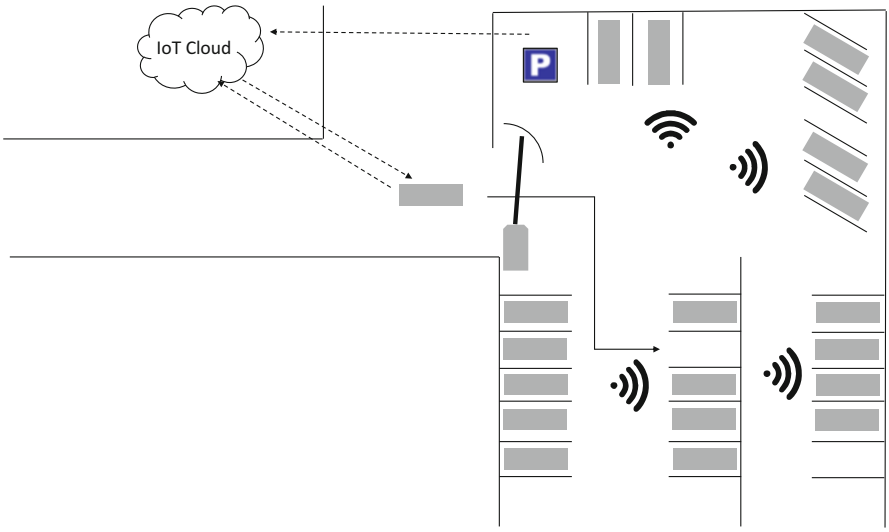

Fig. 10.7 Automated valet parking (AVP) concept of Bosch (see also Nicodemus and Auracher 2015)

The idea is shown in Fig. 10.7 and consists of the following:

- A car can be dropped off at the gate of a parking lot or park house which has been modified to allow AVP.
- The modifications to the parking lot are substantial but only need one time investments.
- The park house uses laser range finders to track cars and sensors in the ground to automatically notify free parking positions.
- The car relies on the onboard parking assistance systems and other ADAS features to control the maneuver (see Chap. 11).
- When the car is identified and allowed to enter the park house, it automatically connects to a WLAN.
- Through this WLAN the car communicates with the park house.
- The car gets the information about where to find a free parking lot and will be guided by the laser range finders and camera systems installed in the parking lot.
- The combination of both onboard sensors and outside sensors (park house infrastructure) increases the safety substantially.
- If the car faces an obstacle, the parking assistance system will automatically stop the car.
- Such a stop command can also come from the parking lot guidance system, if, for example, another car is approaching.
- The valet function will also automatically guide the car from the parking position back to the gate when the driver calls it.

Another AVP solution, called Park4U, is being offered by Valeo (URL33 2017). Park4U relies more on the vehicle sensors and does not need modifications to the parking lot itself. The car is automatically piloted to a free parking space by means of stereo cameras and ultrasound sensors in the vehicle.

The legal framework for automated valet parking, however, still has to be developed fully. Especially the clause of the Vienna Convention on Road Traffic (URL37 2017), that, at any given time the driver needs to be in control (steering, gas pedal, and break), i.e., should be able to step in and drive the car, is a problem. There are multiple initiatives to modify the Vienna protocol to allow for piloted driving. Here, automated valet parking can have a major impact and can be an important step towards full-autonomous driving as the speed of the car is typically low.

Currently, there are various activities in automated valet parking:

- Car2Go and Bosch—cooperation on AVP for carsharing (Gerster 2016; URL24 2017; URL38 2017) as shown in Fig. 10.8.
- BMW Drive Now also plans to introduce AVP. This is based on a hub model, where the car will automatically find back its way. Also, predictive parking algorithms are used to relocate cars.
- Smart city applications and showcases—see Ludwigsburg main station/park house with AVP functionality.
- AutoPles is a research project that demonstrated a proof of concept for combining automated valet parking and automated charging of electric vehicles (URL34 2017). The project partners were Trans Energy Partners, CTC cartech company GmbH, Böblingen, IPT GmbH, Weil am Rhein, Lapp Systems GmbH, Stuttgart, and Research Center for Information Technology (FZI), Karlsruhe.

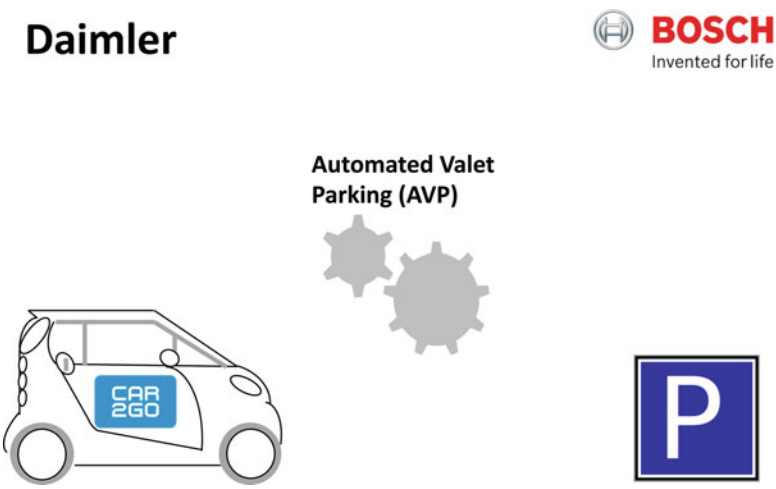

Fig. 10.8 Bosch and Daimler collaborate on automatic valet parking (Gräfe 2016; URL3 2015; URL38 2017)

There are a lot of other pilot projects and research activities going on; however, they are not always visible as automated valet parking is considered to be a highly competitive field, both for OEMs and for x-tiers, alike. A timeline for the introduction of automated valet parking in the overall context of automated, piloted driving, can be found in Freitag (2016).

Carsharing is a particularly promising area for automatic valet parking due to the following reasons:

- Dropping off the car and finding a parking place is a big issue, especially in metropolitan areas.
- Availability of suitable parking places can be the biggest hurdle for efficient use of carsharing.
- AVP allows for up to 20% higher utilization of parking space.
- Combination of parking and charging for shared electric cars is possible (see AutoPles project).

10.5 Cyber Threats

With the digital transformation of the economy, cybercrime, and cybersecurity are topics which make it into the news regularly (Berke 2015; Germis 2016). The cyber threats to connected vehicles are getting more and more attention in the general media, scientific community, and automotive industry (Currie 2015; Gerhager 2016; Greenberg 2013; Lobe 2016; Poulsen 2010; Solon 2015; Stockburger 2016).

Connected parking, remote parking, and automated valet parking solutions are vulnerable to cyberattacks (Chucholowski and Lienkamp 2014). Autonomous features potentially increase the consequences of an attack as the human driver cannot oversee all situations and, if necessary, overpower the machine (Markey 2015; URL30 2017). Cyberattackers could try to steal the car or gain unauthorized access to critical systems. Unauthorized, remote access to the trunk of the vehicle by sending a remote opening command introduces several potential new risks. AVP opens up the possibility of new cyberattack threats mainly due to the need of vehicle-to-infrastructure (V2I) communication with the infrastructure of the park house.

Cyber threats can only be dealt with in a holistic, life cycle-oriented manner that includes HW, SW, and people, like engineers, car owners, dealers, workshop staff, etc. (Besenbruch 2014; Weimerskirch 2016).

The Spy Car Act (Markey 2015; Weimerskirch 2016) has put pressure on the industry to fight against cyber threats and to look at efficient cybersecurity solutions. Quick and efficient responses to cyberattacks and vulnerabilities will be very important in the future (Zetter 2015; Markey 2015), especially with more and more of safety critical functions depending on connectivity (Vembo 2016).

Park house management systems often use a Windows-PC as an industrial park house management system. If the operating system is not patched properly or—worse—support has expired, as in the case of Windows XP, this can be a serious

threat (Haas et al. 2017). Malware could be introduced through the USB port or sent through the network and could compromise the attached subsystems, actuators, and sensors. In such a scenario, vehicles could receive false signals and guidance commands. Also, the in-house position guidance system could be disturbed and rendered useless for path planning.

The major cyber threats to connected parking and automatic valet parking have been outlined in (Haas and Möller 2017):

- Compromising the connection between smartphone/key and vehicle resulting in loss of control of the car, e.g., by man-in-the-middle attacks (Wolf et al. 2016; Wolf and Osterhues 2013).
- Compromising vehicle to infrastructure communication when the car is in transit from the point of dropping it off to the car par or park house.
- Attacks on emergency V2I communication protocols which enable an AVP car to receive commands coming from other top priority traffic participants like ambulance, police, etc. instructing the vehicle to stop and give way. A hacker could exploit this mechanism to gain control.
- The parking management system and car park infrastructure could be hacked by criminal groups trying to gain control of the car while it is out of sight from the owner.
- Attacks could also directly affect the sensors like blinding camera sensors, confusing camera auto control, relaying or spoofing signals, etc.

10.6 Intrusion Detection and Prevention

Intrusion detection systems (IDS) are a mechanism to detect any kind of intrusion into a system. Fallstrand and Lindstrom (2015) define such a system as follows "A system that detects malicious activities, policy violations or other such irregularities in the system and reports them."

Modern automobiles have sophisticated advanced driver assistance functions like intelligent parking assistance, blind-spot detection, lane departure warning, adaptive cruise control, automatic emergency breaking, navigation systems with real-time updates and many more. It is crucial to ensure that these functions behave the way they are supposed to without any outside interference (Haas et al. 2017; Haas and Möller 2017). An IDS can be deployed to detect abnormal behavior, thereby minimizing the effect of cyberattacks exploiting vulnerabilities and malicious tampering with the system (Scarfone and Mell 2007; Serio and Wollenschläger 2015; Weimerskirch 2016; Wolfsthal and Serio 2015).

10.6.1 Types of Intrusion Detection Systems

There are multiple categories and types of intrusion detection systems (IDSs) (Vestlund 2009). The main categories are:

- *Host-based IDS (HIDS)*: This type of system resides on the host and examines the internal state by reviewing the logs of system calls, modification of files, etc.
- *Network-based IDS (NIDS)*: This type of system examines the data traffic between hosts in the network.
- *Hybrid IDS*: This type of system combines the use of HIDS and NIDS on various nodes and hosts for analysis purposes.

Note, that HIDS and NIDS are meant for specific applications only. They cannot be interchanged with one another. Hybrid systems however can be used for any kind of applications and they combine the advantages of HIDS and NIDS.

There are different ways of detecting an intrusion. These can also be applied to a connected car, as it can be seen as a computer network, both internally (networked ECUs) as well as externally as a network of connected cars, and infrastructure. The most important IDS are:

- *Signature-based IDS*: Uses rules to describe malicious behavior in order to detect an intrusion. It compares sequences of events, and patterns to the rules that it has stored in its existing database. The rules can be applied from single to multiple packets. The database needs to be constantly updated with new signatures for different kinds of intrusions. However, if there is a slight change in pattern, the IDS will most likely ignore it. The biggest problem occurs, if the attack does not contain any kind of signature. It will be not updated in the database; hence, the intrusion will be undetected for subsequent access/intrusion.
  - Advantage: Small attacks containing signatures can be easily detected and thwarted.
  - Disadvantage: Attacks without signature cannot be detected.
- *Anomaly-based IDS*: The system creates different profiles of usage over time. The IDS can examine the observed behavior and compare them with the different profiles created. If there is too much deviation from the profiles, then the system reports an intrusion. This can lead to false-positive alarms, depending upon the aggressiveness of IDS. False positives are events that are reported malicious, but in reality they are completely harmless.
  - Advantage: No pre-defined rules for detection of attacks are required; hence, new attacks can be detected.
  - Disadvantage: False-positive cases can arise, leading to confusion for the users. Establishment of normal profile usage is required, which is hard to achieve.

10.6.2 Attacks Against Connected Cars

Like any connected system, connected cars are vulnerable and face some classical attacks known from computer networks. Also, one has to keep in mind that the ECUs of a modern mid-to-high range car, infotainment units, and specialized ECUs for

advanced driver assistance systems (ADAS) (see also Chap. 11), like parking assistance (PA) and automatic valet parking (AVP) (see also Chap. 10), offer much more computational power than a desktop computer. Therefore, different kinds of cyberattacks are possible, such as:

- *Distributed Denial of Service (DDoS)*: This is one of the most serious attacks. A denial of service would prevent a user from accessing network services by clogging up the system resources, thus reducing the efficiency and performance of the network. In the connected car scenario, an attacker could create a large number of fake identities and could transmit dummy messages to a legitimate car to create a jam in the network. A distributed denial of service uses multiple cars from different locations and time slots to carry out the same attack.

  Intrusion detection systems (IDS) can be employed to detect and prevent such attack, by using the anomaly-based method as described in the previous section. The normal utilization of system resources can be setup as a profile, and the behavior of an attack can be monitored against the profile. High deviation would mean that the car is being attacked, and appropriate measures can be taken.
- *Black Hole Attack*. Area where the network traffic is redirected, and there is no subsequent response. The reason could be that there is no node or the node refuses to respond. The attacker's node can fool its neighbors, thus gaining the right to forward the packets. Once the attacker node gets the packet, it can drop it or forward it to an incorrect node. Alheeti et al. (2015a, b) shows how to address this problem by building an intelligent IDS that uses proportional overlapping scores to derive a set of features which describe the normal or abnormal behavior of vehicles. A simple solution includes the packet sequence number in order to identify the packets that have been dropped.
- *Sybil Attack*: Is a very common attack, that occurs by malicious node impersonating them as some legitimate node and then sending wrong messages. In the vehicular context, a vehicle declares to be several other vehicles at the same time or in succession. A vehicle can claim to be in different positions, creating chaos and making the attack very dangerous. It can damage network topologies as well as use a significant amount of network bandwidth (La Vinh and Cavalli 2014). Certain solutions (Xiao et al. 2006) try to detect and localize the position of the Sybil node. They analyze the signal strength distribution and use that to estimate the distance between the Sybil and current node. If the distance measured through signal strength is not the same as being advertised, then the node is likely to be a Sybil node.
- *Bogus Messaging*: This attack can be orchestrated by an attacker or a legitimate user and simply consists of sending false messages in the network. This attack is beyond the scope of IDS. Other cryptographic schemes such as message authentication can be used instead.

- *Timing Attack*: Many functions in a vehicle are time critical (e.g., breaking, powertrain control), which require data transmissions in hard real time. When malicious nodes-/malware-inflicted systems receive a message, they do not forward it immediately but add some time slots to the original message to create a delay. Thus, other subsystems receive the message much later than they were supposed to. In certain cases, this can directly lead to accidents due to the delay of messages. This cannot be detected by signature-based or anomaly-based IDS. Hence, other methods such as data integrity are required to curb such attacks.

10.6.3 Artificial Neural Network-Based IDS Implementation

One way to implement intelligent intrusion detection systems is to use artificial neural networks (ANN) which can be trained to detect and classify malicious activities from the network. The multilayer perception model of an ANN is shown in Fig. 10.9 (see also Chap. 6).

A popular category of an ANN is the multilayer perceptron (MLP for short). These networks consist of nonlinear neurons based on the following activation model (Haykin 2009).

$$y = \sigma\left(\sum_{i=1}^{n} w_i x_i\right) = \sigma(\mathbf{w}^T \mathbf{x})$$

where $x_i \in \mathbb{R}^n$ represents an n-dimensional input vector, which is multiplied with weight factors w_i and mapped to an activation level in the range $[0,1] \subset \mathbb{R}$ by a nonlinear activation function $\sigma(\cdot)$.

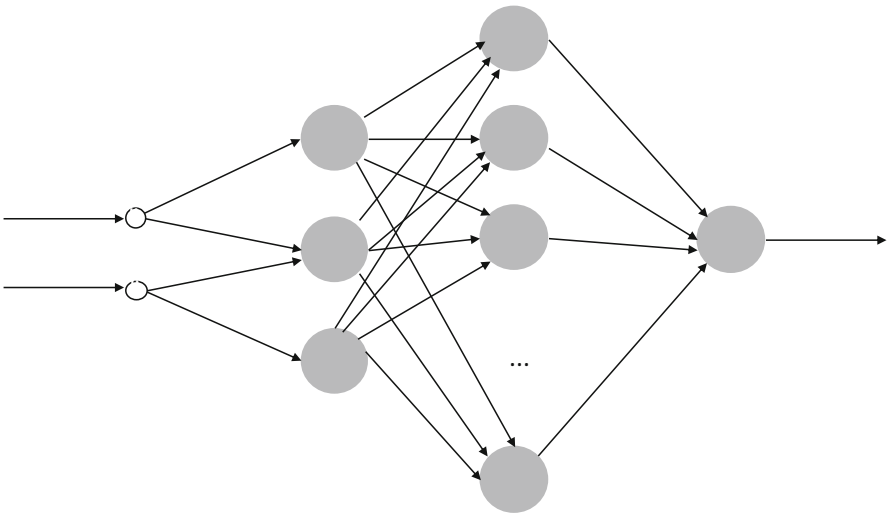

Fig. 10.9 Multilayer perceptron ANN model

The neurons form a multilayer structure, in which the signals of the input neurons are being propagated forward layer by layer. The MLP belongs to the class of feedforward nets.

A difficult design decision is the choice of network layers. While a proof exists that the universal approximation property can be achieved by just one layer, this is only an existence theorem (Haykin 2008). In practice, however, the choice of more layers often leads to more compact and smaller networks.

The first stage in designing ANN-based IDS is the data gathering and pre-processing part. Thus, all incoming data is collected, transformed, and normalized to standard units as illustrated in Fig. 10.10. The next step would be to extract features from this data. Features are characteristics of the data stream that can be measured such as the number of packets transferred (on the vehicle bus systems, between two vehicles, between vehicle and infrastructure, etc.), delay in transfer of packets, number of dropped packets, etc. Other features could be the information in the header of the packets including time-to-live, payload size and type, source and destination MAC, IP address, port, and so on.

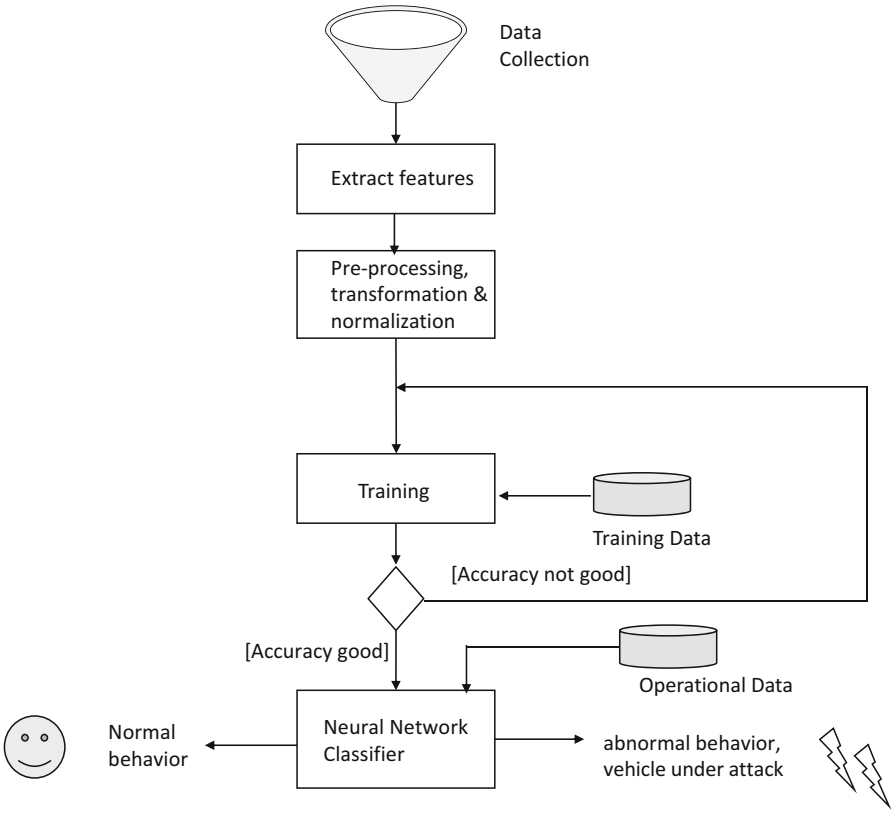

Fig. 10.10 Training of an ANN-based Intrusion Detection System (IDS) (Haas and Möller 2017; Alheeti et al. 2015a, b)

Finally, the trained ANN should be able to recognize and classify the data packets and control messages in the network in real-time as shown in Fig. 10.10. If malicious or abnormal behavior is detected, an alarm can be generated and reported (Alheeti et al. 2015b).

Many automotive manufacturers have taken up the challenge and are currently evaluating sophisticated intrusion detection systems, based on nonlinear classification schemes (like the neural network approach described above) and machine learning algorithms (see Fig. 10.10).

Several companies already offer IDS as commercially available automotive cybersecurity solutions (Serio and Wollenschläger 2015; Weimerskirch 2016; URL1 2015; URL4 2015; URL30 2017; URL36 2017):

- Samsung/Harman/TowerSec
- Continental/Argus
- Bosch/ETAS/ESCRYPT GmbH
- Cisco
- Honeywell
- IBM
- McAfee (formerly with Intel)
- Symantec
- Trilliu

Many first-tier suppliers have strengthened their cybersecurity capabilities through acquisitions, for example, Harman by acquiring TowerSec in 2016.

Figure 10.11 illustrates how an intrusion detection and prevention system (IDS/PS or IDPS for short) can be embedded into the E/E architecture of a modern vehicle. The telematic control unit (TCU) and the central gateway are

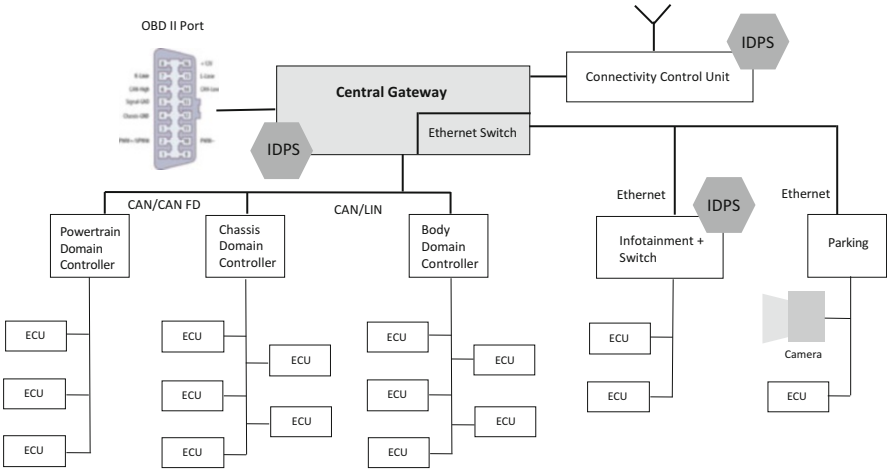

Fig. 10.11 Different options to integrate an IDPS into the E/E architecture and topology of a modern vehicle

straightforward choices for the IDPS, but also the OBD II port, critical ECUs, and high-speed bus systems, for example, Ethernet-based systems for ADAS functionality, can be good choices.

Automotive IDPS should have characteristics like real-time detection, low resource consumption, and continuous data processing. Also, a perfect balance between the computing and memory resources and the performance, detection capabilities, false positives, learning, cost, and quick response capabilities has to be found.

10.7 Conclusion and Recommended Readings

Parking is a difficult and tedious task. The search for available parking space accounts for a major part of inner-city traffic and can lead to a lot of frustration. Accidents while parking are a major cause of damage repair work.

The digital transformation affects the classical business of parking in a major way. Connectivity can help to identify available parking spaces upfront and often in real-time. Many apps are available in the market that allow for finding parking space, booking, and cashless billing; some of them communicate with the infrastructure automatically (opening gates and turnpikes). One can differentiate between on-street parking and off-street parking, e.g., parking lots at airports, shopping malls, or park-and-ride facilities. Parking assistance systems help to maneuver the car even into narrow parking lots. The first generation of systems could only warn, when a car came too close to obstacles; later systems were capable of controlling the lateral position of the car, the current generation of systems can also control longitudinal movements, and the driver just supervises the process. The highest level of automation is automated valet parking which allows the driver to drop off the car, while the car automatically enters the car park and finds a free parking lot. Such systems heavily rely on sensors and car-to-infrastructure communication while the speed is limited, typically to a max of 6 km/h.

10.7.1 Cyber Threats and Cybersecurity

Connected parking exposes many attack surfaces and is prone to cybersecurity threats. This chapter gave an overview of the main problems and discussed a solution based on intrusion detection and prevention. Modern vehicles are fully connected and are prone to cyberattacks as they expose a complex attack surface (see also Chap. 6). Intrusion detection systems can help to detect attacks by filtering the data streams of the connected car and classifying the data into normal or abnormal (i.e., potentially malicious).

This chapter has given a brief overview of the principle of intrusion detection, and we have discussed how these systems can be used to prevent cyberattacks on cars. Intrusion detection systems are based on nonlinear pattern recognition methods. A

popular and well-known way to implement them is to use machine learning, artificial neural networks and deep neural networks (DNNs), as explained in Chap. 6.

10.7.2 Recommended Readings

Balani (2015) gives a good overview of the general concept of an IoT cloud and discusses the IoT solutions of Microsoft Azure, GEs Predix IoT cloud, and Amazons AWS IoT cloud in detail. Mahaffey (2015a, b) emphasizes the importance of a strong collaboration between cybersecurity researchers, automotive OEMs, and technology firms. He sees Tesla as an excellent example of how this collaboration can help to quickly respond to new security threats. Miller and Valasek (2014, 2015) give an in-depth analysis of vulnerabilities and cyberattacks. Miller and Valasek both work for Uber now. Pickhard et al. (2015) emphasize how important it is to focus on data security already in early phases of development. Cryptography plays a key role to secure the communication between cars, infrastructure, and the driver's smartphone (Wolf et al. 2016). Reuss et al. (2015) discuss the synergies between autonomous driving and e-mobility. The integration of AVP and charging will be an important function for electric vehicles in the future. Vembo (2016) gives an overview of the challenges and architecture of connected cars.

In URL1 (2015) a good overview of the key problems in automotive cybersecurity is given. The authors discuss best practices on how to prevent and mitigate cyberattacks. URL2 (2015) looks into the future and poses the question if the steering wheel will be needed at all.

Apart from the parking apps and solution providers discussed in this chapter, there are several others with interesting concepts, for example, ParkJockey (URL6 2017) and EasyPark (URL17 2017).

The IAA auto show in 2017, like in 2015, organized a special exhibition on new mobility. This exhibition provided a platform for start-ups and technology specialists in connected parking (URL28 2017).

10.8 Exercises

What is meant by the term *parking industry*?
Describe the main characteristics of the parking industry.
What is meant by the term *connected parking*?
Describe the main characteristics of connected parking.
What is meant be the term *community-based parking?*
Describe the main characteristics of community-based parking.
What features do you expect from a *connected parking app?*
Describe the main features of a connected parking app.
What methods are being used to *detect a free parking lot?*
Describe the most relevant method to detect a free parking lot.

What is meant by the terms *on-street and off-street parking?*
Describe the main difference between on-street and off-street parking.
What is meant by *predictive parking?*
Give an example for predictive parking.
What are the *parking assistance systems?*
Describe the main features used.
What *sensors are typically being used for parking assistance systems?*
Describe the sensor types used and give an example for the system.
What is meant by the term *remote parking?*
Describe the characteristics, benefits, and challenges of remote parking.
Explain why BMW requires *drivers to constantly press a key while the car parks remotely.*
Explain how the *parking assistance system deals with obstacles in the driving path.*
Explain the *difference between remote parking and automated valet parking*.
What *research initiatives and proofs of concept in AVP are you aware of?*
Describe the main research initiatives and proof of concept used.
What will be the *acceptance of AVP?*
Explain whether there are challenges or not for OEMs to convince their customers to give up the control of the parking process.
Will people *trust technology to park the vehicle?*
Will there be *new players and start-ups entering the AVP market*?
Characterize the new players.
What *demand in the market do you see for AVP?*
Explain your thoughts.
In what *regions and markets will AVP be introduced first?*
Which *markets will follow and what is the timeline?*
How much of a *competitive differentiation will AVP be for OEMs in the future?*
Give an example-based ratio.
What is the *evolutionary path from parking assist to AVP?*
Describe the commonalities and the differences.
What new *business models could emerge for AVP?*
Answer the question w.r.t. funding, location aware services, and parking infrastructure.
What *role will AVP play for carsharing, ridesharing, and electric cars?*
Give examples w.r.t. who will cooperate with whom, OEM, suppliers, and service providers.
What are the *biggest hurdles for introducing AVP from a technology viewpoint?*
Give an example and explain the example in detail.
What *sensors will be used for AVP?*
Describe the sensor types used and give an example for the system.
What is the *relationship of AVP sensors with ADAS and autonomous/piloted driving?*
Give an example and explain the example in detail.
Which *guidelines for the development of semiautonomous vehicles, official standards, and regulations do apply to autonomous parking technologies?*

Give an example and explain the example in detail.
How does the potentially more *predictable environment (light, weather,* etc.*) in a car park influence the required HW/SW?*
Give an example for the HW and SW requirements and explain the example in detail.
Does the car need *access to special sensors inside the parking structure?*
Give an example for the type of sensors and explain the example in detail.
What would be the *cost to set up a parking infrastructure?*
Give your thoughts and explain them.
How will the *car park's management system communicate with the car in order to find and allocate a free parking space and transmit the route to the car. Is this done using GPS or dedicated system/app or Wi-Fi, and how will one deal with weak signals?*
Describe a scenario and explain the chosen constraints.
How does the *human-machine interface (HMI) for AVP look like?*
Describe the scenarios for apps on smartphone, smartwatch, and others.
What are the *biggest obstacles for AVP from a legal viewpoint?*
Describe your thoughts and explain them, and comment on product liability issues in AVP.
What *legal framework is applicable for AVP?*
Describe your thoughts and explain them.
What *modifications are needed in the future?*
Describe your thoughts and explain them.
Can AVP have an *impact on car insurance models?*
Describe your thoughts and explain them.
What kind of *objects can block the path of an AVP system and how can it recognize these objects and avoid accidents in such situations?*
Describe scenarios for another vehicle, a pedestrian, a bicycle, a kid, and an animal.
What are the *cybersecurity concerns in connected parking?*
Describe how an AVP system can be attacked.
What *cybersecurity threats does a connected car face?*
Describe possible attack scenarios.
Why are *connected cars interesting to cybercriminals?*
Describe your thoughts and explain them.
What is meant by the term *intrusion detection system?*
Describe the main characteristics of an IDS and how it can be implemented.
What is meant by the term *artificial neural network?*
Describe the basic principle of an ANN and how the training process can be done.
What other *nonlinear pattern recognition methodologies are you aware of?*
Give examples and describe them in detail.
How to *implement an IDS with a ANN?*
Describe your thoughts and explain them.
What *commercial solutions for IDS are available, and what are the limitations?*
Give examples and describe them in detail.
How does an *automotive IDS differ from a classical computer network IDS?*

Describe your thoughts and explain them.
What *impact will AVP have on the car parking space, especially in city areas?*
Describe your thoughts and explain them.
What role does *AVP play in smart cities?*
Describe your thoughts and explain them.
Are there *social implications of AVP, and how can these implications be compared to the social impact autonomous driving will have?*
Describe your thoughts and explain them.

References and Further Reading

(Alheeti et al. 2015a) Alheeti, K. M. A., Gruebler, A., McDonald-Maier, K. D.: An intrusion detection system against malicious attacks on the communication network of driverless cars. In: Proceedings 12th Annual IEEE Consumer Communications and Networking Conference (CCNC), pp. 916-921, 2015

(Alheeti et al. 2015b) Alheeti, K. M. A., Gruebler, A., McDonald-Maier, K. D.: An Intrusion Detection System against Black Hole Attacks on the Communication Network of Self-Driving Cars. In: Proceedings 6th International Conference on Emerging Security Technologies (EST), pp. 86-91, 2015

(Balani 2015) Balani, N.: Enterprise IoT – A Definite Handbook, Self-published, Kindle Edition, 2016

(Brisbourne 2014) Brisbourne, A.: Tesla's Over-the-Air Fix: Best Example Yet of the Internet of Things? Wired online. February 2014. Available from: http://www.wired.com/insights/2014/02/teslas-air-fix-best-example-yet-internet-things/

(Berke 2015) Berke, J.: Hacker attacks on companies – When cyberattacks lead to bankruptcy (in German). Wirtschaftswoche online. November 25th 2015. Available from: http://www.wiwo.de/unternehmen/it/hackerangriffe-aufunternehmen-wenn-cyberattacken-in-den-bankrott-fuehren/12632916.html

(Besenbruch 2014) Besenbruch, D.: Electronic Systems – Protection against Manipulation (in German), ATZ elektronik, 7/2014

(Chandrasekar et al. 2013) Chandrasekar, P, Barua, N, Zia, Y.: Future of Vehicle Parking Management Systems in North America and Europe. Frost & Sullivan. October 1st 2013. Available from: https://de.slideshare.net/FrostandSullivan/parking-management-26752963

(Chucholowski and Lienkamp 2014) Chucholowski, F., Lienkamp, M.: Teleoperated Driving – Secure and Robust Data Connections (in German). ATZ elektronik, 01/2014

(Currie 2015) Currie, R.: Developments in Car Hacking, December 5th 2015. SANS Institute. Available from: https://www.sans.org/reading-room/whitepapers/internet/developments-car-hacking-36607

(Dierig 2012) Online Parking is too cheap in Germany (in German). Welt online. October 8th 2012. Available from: http://www.welt.de/wirtschaft/article109690967/Parken-ist-in-Deutschland-viel-zu-billig.html

(Fallstrand and Lindstrom 2015) Fallstrand, D., Lindstrom, V.: Automotive IDPS: Applicability analysis of intrusion detection and prevention in automotive systems. Master' Thesis. Chalmers University of Technology. Available from: http://publications.lib.chalmers.se/records/fulltext/219075/219075.pdf

(Freitag 2016) Freitag, M.: Robotic Cars - German Manufacturers in Pole Position (in German). July 26th 2016. Available from: https://www.manager-magazin.de/unternehmen/autoindustrie/roboterautos-deutsche-autobauer-fuehrena-1104783.html

(Gebhardt 2016) Gebhardt, M.: This is how we park tomorrow (in German). Zeit online. May 10th 2016. Available from: https://www.zeit.de/mobilitaet/2016-04/autonomes-fahren-parken-bosch

(Gerhager 2016) Gerhager, S.: Why auto makers might soon get into the focus of blackmailers (in German). Focus online. October 17th 2016. Available from: http://www.focus.de/auto/experten/autoindustrie-warum-autohersteller-fokus-von-erpressern-geraten-koennte_id_6081085.html

(Gräfe 2016) Bosch and Daimler rely on automatic parking searches (in German). Stuttgarter Nachrichten online. March 10th 2016. Available from: http://www.stuttgarter-nachrichten.de/inhalt.stuttgart-bosch-und-daimler-setzen-aufautomatische-parkplatzsuche.6cf6485f-67e5-47f3-817f-8acd5d12e707.html

(Gerster 2016) Assistance systems: Bosch drives automated parking (in German). Automobilwoche, March 2016

(Greenberg 2013) Greenberg, A.: Hackers reveal nasty new car attacks-with me behind the wheel. Forbes online. July 24th 2013. Available from: https://www.forbes.com/sites/andygreenberg/2013/07/24/hackers-reveal-nasty-new-car-attacks-with-me-behind-the-wheel-video/#64771b28228c

(Germis 2016) Germis, C.: Each week 6000 attacks from the Internet against VW (in German). FAZ online. August 18th 2016. Available from: http://www.faz.net/aktuell/wirtschaft/unternehmen/jede-woche-6000-cyberangriffe-gegen-vw-14393188-p2.html#pageIndex_2.8

(Haas et al. 2017) Haas, R., Möller, D., Bansal, P., Ghosh, R., Bhat, S.: Intrusion Detection in Connected Cars. In: Proceed. IEEE/EIT 2017 Conference, pp. 516-519. Ed.: Izadian, A., Catalog No. CFP17EIT-USB 978-1-5090-4766-6, 2017

(Haas and Möller 2017) Haas, R., Möller, D.: Automotive Connectivity, Cyber Attack Scenarios and Automotive Cyber Security. In: Proceed. IEEE/EIT 2017 Conference, pp. 635-639. Ed.: Izadian, A., Catalog No. CFP17EIT-USB. 978-1-5090-4766-6, 2017

(Haykin 2009) Haykin, S.: Neural Network and Learning Machines. 3rd edition. Pearson Education, 2009

(Jungwirth 2016) Presentation of Johann Jungwirth and personal discussion at the Cebit 2017, Hannover, March 2017

(La Vinh and Cavalli 2014) La Vinh, H., Cavalli, A. R.: Security attacks and solutions in vehicular ad hoc networks: a survey. In: International Journal on AdHoc Networking Systems (IJANS), Vol 4, No. 16, pp. 1-20, 2014

(Laudon et al. 2010) Laudon, K., Laudon, J., Dass, R.: Management Information Systems, Pearson Publ., 2010

(Lobe 2016) Lobe, A.: Hacker Alert – In a modern car today are computers and info systems that are easy to manipulate. How do the manufacturers deal with the security gap? (in German). Zeit online. August 25th 2016. Available from: http://www.zeit.de/2016/34/elektroautos-steuerung-hacker-gefahr-sicherheit-hersteller

(Mahaffey 2015a) Mahaffey, K.: The New Assembly Line: 3 Best Practices for Building (secure) Connected Cars. Lookout Blog. August 6th 2015. Available from: https://blog.lookout.com/tesla-research

(Mahaffey 2015b) Mahaffey, K.: Here Is How To Address Car Hacking Threats. TechCrunch. September 13th 2015. Available from: https://techcrunch.com/2015/09/12/to-protect-cars-from-cyber-attacks-a-call-for-action/

(Markey 2015) Markey, E.J.: Tracking and Hacking: Security and Privacy Gaps Put American Drivers at Risk. 2015. Available from: https://www.markey.senate.gov/imo/media/doc/2015-02-06_MarkeyReport-Tracking_Hacking_CarSecurity%202.pdf

(Miller and Valasek 2014) Miller C., Valasek C.: A Survey of Remote Automotive Attack Surfaces. IOActive 2014. Available from: https://www.ioactive.com/pdfs/IOActive_Remote_Attack_Surfaces.pdf

(Miller and Valasek 2015) Miller, C., Valasek, C.: Remote exploitation of an unaltered passenger vehicle. August 10th 2015. Available from: http://illmatics.com/Remote%20Car%20Hacking.pdf

(Min and Choi 2013) Min, K-W., Choi, J-D.: Design and implementation of autonomous vehicle valet parking system. In: Proceedings 16th International IEEE Conference on Intelligent Transportation Systems – (ITSC 2013), 2013

(Nicodemus and Auracher 2015) Connected Parking. EPoSS Workshop on Smart Systems Integration. June 19th 2015. London. Available from: http://www.ivu-bw.de/pdfs/2015/1/DEKRA_ConnectedParking_2015-05-19_Download.pdf
(Pickhard et al. 2015) Pickhard, F., Emele, M., Burton, S., Wollinger, T.: New thinking for safely networked vehicles (in German). ATZ elektronik, 7/2015
(Poulsen 2010) Poulsen, K.: Hacker disables more than 100 cars remotely. Wired online. March 17th 2010. Available from: www.wired.com/threatlevel/2010/03/hacker-bricks-cars
(Rees 2016) Rees, J.: Mobility – Never have to park yourself (in German). Wiwo online. May 6th 2016. Available from: https://www.wiwo.de/technologie/mobilitaet/mobilitaet-nie-mehr-selber-einparken-muessen/13529696.html
(Reuss et al. 2015) Reuss, H.-C., Meyer, G., Meurer, M.: Roadmap 2030 Synergies of Electromobility and Automated Driving (in German). ATZ Elektronik, 7/2015
(Scarfone and Mell 2007) Scarfone, K., Mell, P.: Guide to Intrusion Detection and Prevention Systems (IDPS). NIST. February 20th 2007. Available from: https://www.nist.gov/publications/guide-intrusion-detection-and-prevention-systems-idps
(Serio and Wollschläger 2015) Serio, G., Wollschläger, D.: Networked Automotive Defense Strategies in the Fight against Cyberattacks (in German). ATZ elektronik, 06/2015
(Solon 2015) Solon, O.: From Car-Jacking to Car-Hacking: How Vehicles Became Targets For Cybercriminals. August 4th 2015. Bloomberg online. Available from: https://www.bloomberg.com/news/articles/2015-08-04/hackers-force-carmakers-to-boost-security-for-driverless-era
(Stockburger 2016) Stockburger, C.: IT security of cars: You have no choice but to trust the manufacturers (in German). Spiegel online. November 1st 2016. Available from: http://www.spiegel.de/auto/aktuell/hacker-angriffe-man-hatkeine-andere-wahl-als-den-autoherstellern-zu-trauen-a-1092224.html
(Vembo 2016) Vembo, D.: Connected Cars – Architecture, Challenges and Way Forward. Whitepaper Sasken Communication Technologies Pvt. Ltd. 2016. Available from: https://www.sasken.com/insights/white-papers/connected-cars-–-architecture-challenges-and-way-forward-0
(Vestlund 2009) Vestlund, C.: Intrusion Detection Systems in Networked Embedded Systems. Linköping University. Available from: https://pdfs.semanticscholar.org/10f9/455dde5674de051ae065f358b922cf8bec0f.pdf
(Weimerskirch 2016) Weimerskirch, A.: Cybersecurity for Networked and Automated Vehicles (in German). ATZ elektronik, 03/2016
(Werle 2015) Werle, K.: World in digital change – the game changer – BMW smartphone on wheels (in German). Manager Magazin. November 23rd 2015. Available from: http://www.manager-magazin.de/unternehmen/artikel/gamechanger-bmw-sieger-in-wettbewerb-von-bain-und-mm-a-1063812.html
(Wolf and Osterhues 2013) Wolf, M., Osterhues, A.: Secure Messages – Modern Cryptography for Protecting Control Devices (in German). ATZ elektronik, 02/2013
(Wolf et al. 2016) Wolf, A, Greiff, S., Obermaier, R.: Vehicle access systems of tomorrow (in German). ATZ Elektronik 03/2016
(Wolfsthal and Serio 2015) Wolfsthal, Y., Serio, G.: Made in IBM Labs: Solution for Detecting Cyber Intrusion to Connected Vehicles, Part I. Available from: https://securityintelligence.com/made-in-ibm-labs-solution-for-detecting-cyber-intrusions-to-connected-vehicles-part-i/
(Xiao et al. 2006) Xiao, B., Yu, B., Gao, C.: Detection and localization of Sybil nodes in VANETs, in DIWANS 06, Los Angeles, CA, pp. 1–8, 2006.
(Zetter 2015) Zetter, K.: Researchers Hacked A Model S, But Tesla's Already Released A Patch. Wired online. August 6th 2015. Available from: https://www.wired.com/2015/08/researchers-hacked-model-s-teslas-already/

Links

2014

(URL1 2014) https://www.cisco.com/c/dam/en_us/solutions/industries/docs/parking_aag_final.pdf

2015

(URL1 2015) https://www.mcafee.com/enterprise/en-us/assets/white-papers/wp-automotive-security.pdf
(URL2 2015) https://www.wiwo.de/unternehmen/auto/digitalisierung-der-autoindustrie-kuenftig-braucht-man-das-lenkrad-nicht-mehr/v_detail_tab_print/11602152.html
(URL3 2015) https://www.bosch-presse.de/pressportal/de/en/bosch-and-daimler-automate-parking-mercedes-with-built-in-valet-42989.html
(URL4 2015) https://www.symantec.com/content/dam/symantec/docs/white-papers/building-comprehensive-security-into-cars-en.pdf
(URL5 2015) https://www.congress.gov/bill/114th-congress/senate-bill/1806/all-info
(URL6 2015) https://www.cisco.com/c/en/us/solutions/industries/smart-connected-communities/city-parking.html
(URL7 2015) https://www.digitaltrends.com/cars/bmw-automated-parking-technology-ces-2015/
(URL8 2015) http://www.theiet.org/sectors/transport/documents/automotive-cs.cfm
(URL9 2015) https://newmobility.world/de/

2016

(URL1 2016) http://news.sap.com/sap-iot-seeks-better-parking-with-new-solution/

2017

(URL1 2017) https://en.wikipedia.org/wiki/Parking
(URL2 2017) https://en.parkopedia.com
(URL3 2017) https://parkpocket.com
(URL4 2017) https://www.streetline.com
(URL5 2017) http://inrix.com
(URL6 2017) https://www.parkjockey.com/
(URL7 2017) https://www.tomtom.com/
(URL8 2017) https://spothero.com/
(URL9 2017) https://www.parkwhiz.com/
(URL10 2017) https://www.parkingpanda.com/
(URL11 2017) www.bestparking.com/
(URL12 2017) https://www.parkme.com/
(URL13 2017) https://www.park-now.com/
(URL14 2017) www.gottapark.com/
(URL15 2017) https://www.justpark.com/
(URL16 2017) https://www.ampido.com/
(URL17 2017) https://easyparkgroup.com
(URL18 2017) http://parknav.com

(URL19 2017) https://www.cleverciti.com/
(URL20 2017) https://www.park1.com
(URL21 2017) https://apcoa.com
(URL22 2017) https://www.q-park.com
(URL23 2017) http://www.contipark.de/de-DE/
(URL24 2017) http://www.bosch-mobility-solutions.com/en/highlights/connected-mobility/connected-and-automated-parking/
(URL25 2017) https://www.bosch.com/
(URL26 2017) https://www.bosch.com/explore-and-experience/connected-parking-success-factor-development/
(URL27 2017) https://www.bosch-iot-suite.com/
(URL28 2017) https://www.iaa.de/
(URL29 2017) http://park-here.eu
(URL30 2017) https://argus-sec.com
(URL31 2017) http://www.mobility.siemens.com/mobility/global/en/urban-mobility/road-solutions/integrated-smart-parking-solution/pages/integrated-smart-parking-solution.aspx
(URL32 2017) https://en.wikipedia.org/wiki/INRIX
(URL33 2017) http://www.valeo.com/en/park4u-automated-parking/
(URL34 2017) http://www.emobil-sw.de/en/activities-en/current-projects/project-details/autoples-automated-parking-and-charging-of-electric-vehicle-systems.html
(URL35 2017) https://www.slideshare.net/FrostandSullivan/parking-management-26752963
(URL36 2017) http://www.trillium.co.jp
(URL37 2017) https://en.wikipedia.org/wiki/Vienna_Convention_on_Road_Traffic
(URL38 2017) http://www.bosch-presse.de/pressportal/de/de/bosch-und-daimler-zeigen-fahrerloses-parken-im-realen-verkehr-116096.html