An Overview on Vehicular Communication Standards

Kilian Zieglowski, Holger Kinkelin*
*Chair of Network Architectures and Services, Department of Informatics
Technical University of Munich, Germany
Email: kilian.zieglowski@tum.de, kinkelin@net.in.tum.de

***Abstract*—Communication between vehicles is evolving. It can be used for reducing dangerous situations, improving safety in traffic as well as making driving more convenient by enabling improved in-car entertainment such as Wifi and Video streaming. The main advantage is safer traffic with the goal of reducing traffic collisions to almost zero.**

There are two main techniques and standards that compete in the European market. These are the *C-ITS (Cooperative Intelligent Transport System)* of the EU based on the IEEE 802.11p standard, and the new developing cellular techniques using LTE and in the future the 5G radio standard. This paper shows an overview of the C-ITS and the cellular-based *ITS (Intelligent Transport System)* and its current standardised security architecture. C-ITS is mature and tested, whereas cellular ITS has multiple possible advantages for the future. However, cellular-based ITS still needs to be standardised and tested for vehicle communication.

***Index Terms*—V2X, V2V, C-ITS, IEEE 802.11p, cellular ITS, ITS Security**

1. Introduction

The *IoT (Internet of Things)* is becoming an important part of our lives. More and more things are connected and becoming smarter. Meanwhile, IoT is even used in the automotive industry with the aim to make our transportation safer and more comfortable. This means making cars smarter and enabling them to communicate with each other in real-time. [1]

The new technology is called *V2X (Vehicle to Everything)* communication which is the summary of four different communication types [2]. These types are *V2V (Vehicle to Vehicle)*, *V2I (Vehicle to Infrastructure)*, *V2P (Vehicle to Pedestrian)* as well as *V2N (Vehicle to Network)* [2]. The V2X *ITS (Intelligent Transport System)* has four primary purposes [3]. First, ITS can be used for improving the safety of transportation with, e.g. assistance and warnings [4]. The primary purpose is to react on the not line of sight area, where the current sensors of a car are nowadays useless [5]. Second, ITS can be utilised to optimise traffic flow, e.g. platooning, which is the ability to link vehicles together in an automated way. [4]. Third, it can also be used for better in-car entertainment for business or pleasure by offering video-streaming or Wifi for mobile devices [6]. Fourth, autonomous driving can be improved with V2X, so a vehicle knows where the others are located, what they see and has the ability to predict the next most likely situation [3].

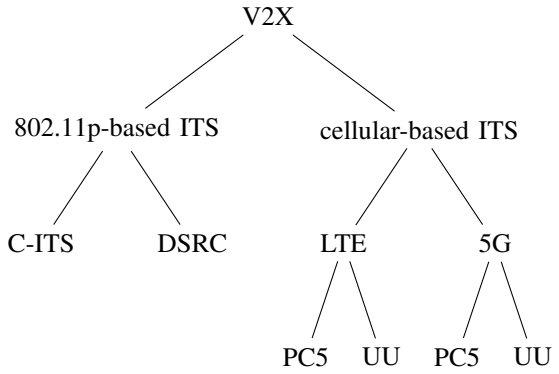

Figure 1: Taxonomy of used V2X communications

The V2X communication can be split into three leading technologies divided into two fields, which can be seen in figure 1. One field is the 802.11p-based standard, with the two technologies *DSRC (Dedicated Short Range Communication)* of the USA and the *C-ITS (Cooperative Intelligent Transport System)* of the EU [4]. Another field and technology is the cellular-based system. It uses for short direct communication the PC5 and for far infrastructure communication the UU interface, in LTE and the upcoming 5G standard [4].

The aim of this paper is to give an overview which will include advantages and disadvantages of the IEEE 802.11p-based communication, with a special focus on C-ITS in Section 2, which will be followed by LTE/5G-based communication in Section 3. Furthermore, opportunities and difficulties of the coexistence of LTE-based and IEEE 802.11p-based ITS are detailed in Section 4. In Section 5, the security is described with the features of IEEE 802.11p-based ITS in Subsection 5.1 as well as of the LTE-based ITS in Subsection 5.2. In Section 6, some related work is listed, which is followed by the conclusion in Section 7.

2. IEEE 802.11p-based ITS

IEEE 802.11p is based on the normal Wifi standard IEEE 802.11a, which is broadly used in private Wifi environments and is adapted for the use in V2X communication [5]. The V2V communication based on the Wifi Standard 802.11p standard is mature and well tested, which makes it a technique ready to use [7]. The 802.11p is divided into two primary standards: the DSRC of the USA and the C-ITS of the EU [4].

doi: 10.2313/NET-2020-04-1_11

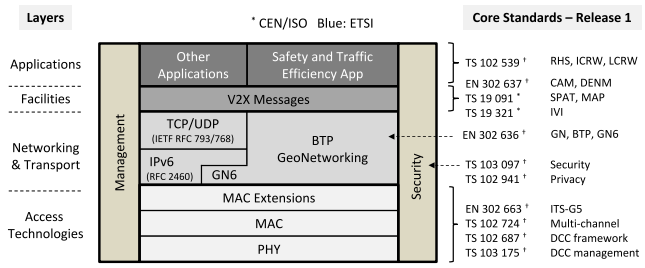

Figure 2: C-ITS protocol stack and standards [4]

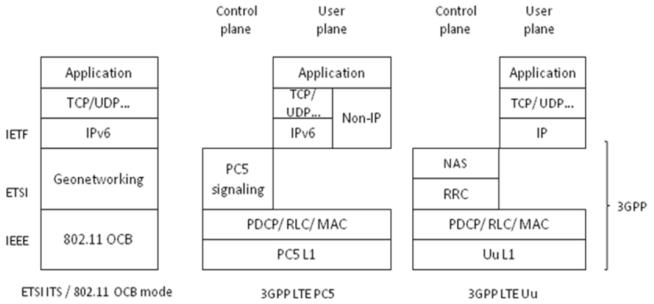

Figure 3: Protocol stack and standards for LTE-UU and PC5 in comparison to C-ITS [13]

In the following, the focus is set on the C-ITS of the EU, because of multiple similarities between DSRC and C-ITS. The idea of the C-ITS was to spread information about, e.g. speed and direction to vehicles nearby and if necessary use multi-hop to reach afar vehicles [4]. Moreover, the EU wants to develop the ITS system without any infrastructure with the main focus on V2V communication [8]. It can be seen as a network of vehicles communicating with each other and relaying messages. This network decreases the expenses of each car owner by excluding costly infrastructure. However, for effective usage, a minimum of 10% of all the cars need to be equipped with the ITS system to have a noticeable impact on safety [8]. This equipment quantity would be reached in 2.5 years if every second newly released vehicle would be equipped with C-ITS [8].

C-ITS operates like DSRC in the 5 GHz frequency band and uses the same technology in the lower PHY and MAC protocol layer [4], which can be seen in figure 2. The single-hop communication ranges from 10 metres up to 1 kilometre depending on the weather conditions and if it is in line of vision [4]. The communication can be further extended by multi-hop message transport [4]. The multi-hop communication uses geographical data for effective routing [4]. This routing is needed because not every vehicle in range should resend each message [4]. Such a resending of every vehicle in proximity could lead to an overhead and breakdown of the system [4]. Therefore, the selection of vehicles utilises an algorithm, which uses the broadcast information from the vehicles about their location and their neighbours [4].

Furthermore, the channel width is reduced to 10Mhz, as a result of robustness issues [8]. That limits the communication data rates to 27 Mb/s, which can be reduced to 3 Mb/s to react to interferences and enable a larger communication range and a lower packet failure rate [8]. Nevertheless, this low data rate limits the usability in the entertainment segment, e.g. video streaming of the infrastructure or gaming between vehicles [8]. Moreover, 802.11p has a high potential of errors in high-density vehicle conditions, no exact future enhancement plans, or usable and buildable *RSUs (Road Side Units)* [7]. However, for safety-relevant communication it is crucial to support a low latency real-time communication and C-ITS enables typical end to end latencies of under 10 ms [9].

802.11p is adapted to the high mobility in vehicle communication, with a maximum operating speed of 500 km/h by handling doppler effects and frequent changing multi-path reflections [5]. Notwithstanding, there are scalability issues in high-density areas such as traffic jams because just a single device is capable of sending a package in a certain time and channel in DSRC [10].

3. Cellular-based ITS

The use of LTE for V2X communication is still immature and so far not ready to use, but it has multiple advantages today and in future [7]. One aspect is the steady development and improvement of specifications and capabilities of the general cellular standards, which are the basis for cellular V2X communication [7]. The main advantage of cellular-based communication is the already existing infrastructure [4] with a global deployment [3]. The quality of service is guaranteed by cellular providers, which offer and enlarge their infrastructure for other use cases such as smartphones. Nearly every new vehicle uses the cellular network and has already the infrastructure on board for, e.g. traffic information [11]. Most manufacturers offer information systems such as *RTTI (Real Time Traffic Information)* which provide data about, e.g. road usage, defect cars or tailbacks [11] for safety and non-safety relevant information.

By developing LTE and *LTE-A (LTE Advanced)*, it evolved to be a worthy competitor for the 802.11p. LTE-A supports a mobility speed of up to 350 km/h, a maximum data rate of 1 Gb/s and a range of up to 30 kilometres [12] and for the first time a direct communication between devices [3].

V2I/V2N communication is realised by the LTE-UU interface [3]. By enabling *D2D (Device to Device)* in LTE-A [3], a direct V2V communication is possible on the basis of a PC5 interface [14]. In LTE Advanced Release 12 of 3GPP, LTE-Direct was supported for the first time and made direct communication between devices in proximity possible [15]. The cooperation 3GPP standardises different standards for LTE-UU and PC5 such as the ETSI does for the C-ITS a comparison can be seen in figure 3. The authentication and timing are initialised via the infrastructure [15]. After that, the devices can communicate directly [15]. The D2D communication is also possible if there is no base station in range or if it is damaged [16]. This extends the working area and saves battery power [16]. However, the D2D system was still insufficient and unspecialised for vehicle speed, so in Release 14 of 3GPP it got adapted to the requirements of V2V communication [16]. Furthermore, the cellular V2X system is capable of integrating other entities such as pedestrians which enables V2P communication

doi: 10.2313/NET-2020-04-1_11

in their system by using the PC5 interface and LTE smartphones [17]. The integration would be beneficial, especially for urban areas with the aim of smart cities [17].

By the use of 5G and its adaption for the communication between machines, the latency of 10 ms to 100 ms of previous generations decreases to 1 ms, as a result of complex back coupling [18]. 5G also enables peak data rates faster than 10 Gb/s, and it supports more than 1 million devices per square kilometre [15]. Moreover, 5G will support a maximum mobility speed of 500 km/h [19]. That means it would also be possible to transport security-relevant information using the new cellular standard.

In future, the LTE module in cars can be replaced with an LTE module which enables both V2V by PC5 and V2I by LTE-UU with only one Chip [17]. The LTE network can handle a high density of devices since it is capable of frequency-domain multiplexing of many devices [10].

4. Coexistence of LTE-based and IEEE 802.11p-based ITS

802.11p, as well as the LTE PC5 standard, are operating on the 5 GHz simultaneously, which would lead to interferences [6]. The *5G Automotive Association (5GAA)*, which support the cellular-based standard, and *car to car communication consortium (C2C-CC)*, which support the WIFI-based communication, are in contact for developing a method so that both technologies can coexist without interferences or malfunctions [15]. 5GAA made a proposal to separate the frequencies among them, which has been rejected by the C2C-CC because the proposed frequencies are used by them [15]. Also, it is crucial to be prepared for prospective challenges and not to rule out one system [15]. Nevertheless, the coexistence of the two systems would be more expensive than just integrating and developing a single one [17].

5. Security

Security is essential for every ITS system because it is processing critical data. Moreover, it is important that every authentication method is able to exclude devices out of the network, which are sending wrong data.

Currently, there are just a few cars which allow direct V2V communication [15] like the new VW Golf 8 [20]. Consumer acceptance is a crucial point that needs to be considered for the integration of ITS. Therefore, it needs to comply with safety and privacy requirements. For secure V2X communication, it is necessary that authentication, authorisation, availability, data confidentiality and data integrity need to be fulfilled to be prepared for all possible types of attack [3]. Finally, it is much needed for privacy reasons to anonymise the data communication so that personal data is secure, and users can not be traced [3].

5.1. IEEE 802.11p-based ITS

In C-ITS the authentication can mainly be separated into two parts, the direct V2V communication and V2I communication. DSRC uses *WAVE (Wireless Access in Vehicular Environments)* which is the combination of IEEE 802.11 and IEEE 1609 standard [4]. IEEE1609.2 defines an authentication method which is useful for V2I [21]. Furthermore, it provides secure communication standards with the use of *PKI (public key infrastructure)* [22]. A *CA (certificate authority)* validates identities and signs certificates [21]. Those certificates can be transferred via DSRC as well as be used for the authentication of messages [21].

In the EU, the security standard for V2X communication is standardised by the ETSI [21]. In the C-ITS, secure access is handled similarly to DSRC and is just broader because of the used GeoNetworking for multi-hop messages [21]. The C-ITS uses as network protocol IPv6 in combination with UDP and TCP as transport protocol [4].

Certificates are also used to support security and privacy [23]. PKI can be used for signing messages, as well with pseudonyms for privacy reasons, to enable secure communication for V2X [23]. The Root-CA is superordinated, which gives certificates to every sub-CA or *EE (End Entity)* [23]. There are at least two sub-CAs: the *EA (Enrollment Authority)* and *AA (Authorisation Authority)* [23]. Each vehicle has a personal signature and a static public key for initialisation whereby the vehicle gets an *EC (Enrollment Credential)* certificate of the EA, which is valid for a few years [23]. An EC is updated shortly before it expires using the still valid EC at EA for verification [23]. Furthermore, the EC of the EA can be used to get short-living *ATs (Authorisation Tickets)* of the AA for the usage between vehicles and infrastructure [23]. The vehicle sends a request to the AA as well as the EC to the EA [23]. If the EC is valid, the EA sends the confirmation to the AA, which gives ATs to the vehicle [23]. For safety reasons, a *CRL (Certificate Revolution List)* is used for revoking access to the system for possible malicious entities, where the ECs are listed [23]. If the EC is not valid, the certificate is sent to the CRL [23]. The separation of authentification of EE in EA and the certificate issuance of AA to EE is for anonymising the exact identity of users, so they can not be traced [23]. The EA saves data of the vehicles for identification on which the AA has no access to [23].

In future, there will be a certificate policy with some requirements for the certificates, but every CA can add requirements for its use [23]. There will be multiple CAs in Europe, and for coordinating certificates between all European countries *TLM (Trust List Manager)* will be used [23]. The TLM lists all certificates so that vehicles can be validated in other states and CAs [23]. The TLM list itself is secured by a certificate with a public key which has to be sent to every entity to get access to the list of all valid certificates in order to communicate with each other [23].

The certificate in a *CAM (Cooperative Awareness Message)* can be reduced to an 8-bit hash code for reducing the load on the communication channel [23]. Furthermore, the hash code and the certificate are saved by the receiver and is updated only once every second [23]. When receiving a message, the hash code is used for verification [23]. CAMs are sent periodically and frequently [23]. The data of CAMs, e.g. speed, position and steering of the own and neighbours vehicles are exchanged regularly and collected in a local dynamic map [23].

GeoNetworking uses the information about the po-

doi: 10.2313/NET-2020-04-1_11

sitions of vehicles for efficient routing [4]. Besides, it enables an exchange of information in a specific geographical area in order not to be restricted by the signal range of a single-vehicle [4]. For transmitting IPv6 packets using GeoNetworking, a sublayer *GN6 (IPv6 over GeoNetworking)* was standardised [4].

A *DENM (Decentralised Environmental Notification Message)* can make multi-hop and is sent in potentially dangerous situations [23]. Those Situations may be, e.g. obstacles on roads, adverse weather conditions or road works [23]. DENMs can be resent and updated in case of longer-lasting dangerous activities and are cancelled when there is no more danger [23]. DENMs are event-driven and are sent when something happens and are not sent regularly in comparison to CAMs [23].

The lower protocol layers PHY and MAC are not expected to be modified in the future so that the suboptimal performance may stay the same [4]. However, it will be modified in the upper layers by superior algorithms for spreading information, with an increase in safety and performance [4].

ECDSA (Elliptical Curve Digital Signature Algorithm) [24] is specified as the signature algorithm, with the usage of the NIST P256, which is an elliptical curve [23]. In future, different algorithms are needed to provide security like the Brainpool curve with 256 or 384-bit length [23]. These are standardised in the ETSI standard TS 103 097 [23].

5.2. Cellular-based ITS

LTE has some standard security mechanisms, but they are not sufficient in a V2V direct communication using the PC5 interface without using the base station [16]. Therefore, the security mechanisms can be divided into two main parts, the direct communication via the PC5 interface and the communication with the infrastructure via the UU interface, and a future enhancement in 5G.

The LTE system can be used for V2N communication. However, vehicles have to be authenticated by the infrastructure and authorised for V2X communication as well as the vehicle has to authenticate the infrastructure [3]. For secure communication of V2X service, the *LTE-AKA (LTE Authentication and Key Agreement)* protocol is used, which is provided by the LTE security framework [3]. LTE-AKA protocol is used for identification, authorisation and key sharing and derivation for facilitating secure wireless access [3]. Nevertheless, the present LTE-AKA is not adapted to, e.g. the high mobility of V2I communication which leads to longer transmission and end-to-end latency times [3]. Additionally, in LTE-AKA the specific identity of the entity is not hidden [3]. Hence, the entities are traceable, and it is possible that a malicious entity uses a man-in-the-middle attack between the vehicle and the infrastructure by using his identity and sending wrong data [3]. This can lead to misinterpretation of vehicles and can result in crashes [3]. Therefore the LTE-AKA protocol has to be further extended for safer, faster and anonymous communication.

Similar to V2I communication, mutual authentication between the vehicles is needed to avoid malicious spread of information [3]. For V2V authentication of communication in the PC5 interface, the ProSe security framework can be used [3]. Furthermore, the ProSe D2D of 3GPP communication can be utilised for authorisation, authentication and discovery [3]. Some differences are that vehicles do not have electricity or computing capacity issues like other mobile devices, what ProSe was initially developed for, but they have a high mobility [3]. Hence, a secure access and communication method specialised for vehicles still need to be standardised [17].

In comparison to that, 5G has multiple use cases and therefore needs a flexible authentication method which supports the variety of requirements [25]. The 5G frequency will support an optimised direct communication for vehicles, where the special security mechanisms of the LTE D2D can be extended [3]. The secure access can be divided into two securing ranges. The first mandatory authentication is for general access to the core 5G [3]. The second authentication will be optional, which is based on protocol configuration options, where the PAP/CHAP user credentials are listed [3].

There are a lot of different techniques to enable secure communication and authentication. Some mechanisms would use the *DHKE (Diffie-Hellman Key Exchange)* generation of symmetric keys or shared keys for a V2I communication [2]. Lastly, TLS or SSL can be used for secure communication, but a distinct disadvantage is that the identity of the entity is visible, which leads to privacy issues [2].

6. Related Work

Beside the C-ITS system of the EU and the cellular-based ITS system, which are explained in this paper, some more systems for ITS are in the development phase. Some other nations made their own tests on ITS such as Australia, Japan, China or South Korea [15]. Furthermore, there is another technology tested for ITS, the *WiMAX (Worldwide Interoperability in Microwave Access)*, but with an insignificant role in the market [3] [26]. Moreover, other countries have their own system and use other frequencies like Japan, which develops an ITS system similar to DSRC of the US [27] [8]. Some other technologies, for example, visible light communication or mmWAVE, were also tested for ITS [15].

7. Conclusion

Both the C-ITS and the cellular-based ITS have advantages and disadvantages. The C-ITS is a mature technology which is ready to use. It offers direct V2V communication as well as V2I, which has small latencies. Furthermore, it allows for more extensive communication ranges the use of equipped vehicles in the middle as a repeater. However, up to now, there is no existing infrastructure on which the system could build on. Moreover, there are no RSUs which are ready to build. Nevertheless, this technology is ready to be published and spread and could save our lives soon.

On the other side, the cellular-based ITS uses the already existing infrastructure which is used for, e.g. smartphones and enables a faster impact on safety, because of this infrastructure. Additionally, it provides the

new PC5 interface, which allows a direct device communication and therefore is a strong competitor for C-ITS. Besides allowing standard cellular communication by using an infrastructure, it also offers a V2V or V2P direct communication. This direct communication reduces the latency time, which was a significant disadvantage for cellular-based ITS. Furthermore, it enables communication where no infrastructure is needed, and it enables communication in areas with insufficient cellular coverage or outdated technology standards, which would have large latencies. However, the cellular-based standard for ITS is not fully standardised and not ready to use, e.g. it has some uncertainties in the secure access control, which will take some time for advancement.

The integration of pedestrians over smartphones is a substantial benefit of cellular-based communication, which would enable the integration of vulnerable roadside users such as pedestrians or cyclists. Beyond that, the ability to use smartphones for communicating with vehicles enables the integration of old cars. The C-ITS would need RSUs for communication with other devices, whose infrastructure was not initially planned by the EU.

References

[1] H. Holland, *Connected Cars*. Wiesbaden: Springer Fachmedien Wiesbaden, 2019, pp. 51–81. [Online]. Available: https://doi.org/10.1007/978-3-658-22929-0_3

[2] K. J. Ahmed and M. J. Lee, "Secure LTE-Based V2X Service," *IEEE Internet of Things Journal*, vol. 5, no. 5, pp. 3724–3732, Oct 2018.

[3] M. Muhammad and G. A. Safdar, "Survey on existing authentication issues for cellular-assisted V2X communication," *Vehicular Communications*, vol. 12, pp. 50 – 65, 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S2214209617302267

[4] A. Festag, "Standards for vehicular communication—from IEEE 802.11p to 5G," *e & i Elektrotechnik und Informationstechnik*, vol. 132, no. 7, pp. 409–416, Nov 2015. [Online]. Available: https://doi.org/10.1007/s00502-015-0343-0

[5] A. Filippi, K. Moerman, V. Martinez, A. Turley, O. Haran, and R. Toledano, "IEEE802. 11p ahead of LTE-V2V for safety applications," *Autotalks NXP*, 2017.

[6] N. Xia and C.-S. Yang, "Vehicular Communications: Standards and Challenges," 2017.

[7] A. Bazzi, B. M. Masini, A. Zanella, and I. Thibault, "On the Performance of IEEE 802.11p and LTE-V2V for the Cooperative Awareness of Connected Vehicles," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 11, pp. 10 419–10 432, Nov 2017.

[8] R. K. Schmidt, T. Leinmüller, and B. Böddeker, "V2x kommunikation," in *In Proceedings of 17th Aachener Kolloquium*, 2008.

[9] C. Ress and M. Wiecker, "Potenzial der V2X-Kommunikation für Verkehrssicherheit und Effizienz," *ATZ - Automobiltechnische Zeitschrift*, vol. 118, no. 1, pp. 16–21, Jan 2016. [Online]. Available: https://doi.org/10.1007/s35148-015-0154-y

[10] H. Seo, K. Lee, S. Yasukawa, Y. Peng, and P. Sartori, "LTE evolution for vehicle-to-everything services," *IEEE Communications Magazine*, vol. 54, no. 6, pp. 22–28, June 2016.

[11] (2019). [Online]. Available: https://www.bmw-me.com/en/topics/fascination-bmw/connected-drive/rtti.html

[12] G. Araniti, C. Campolo, M. Condoluci, A. Iera, and A. Molinaro, "LTE for vehicular networking: a survey," *IEEE Communications Magazine*, vol. 51, no. 5, pp. 148–157, May 2013.

[13] T. Yoshizawa and B. Preneel, "Survey of security aspect of v2x standards and related issues," in *2019 IEEE Conference on Standards for Communications and Networking (CSCN)*, Oct 2019, pp. 1–5.

[14] Y.-L. Tseng, "LTE-advanced enhancement for vehicular communication," *IEEE Wireless Communications*, vol. 22, no. 6, pp. 4–7, 2015.

[15] B. Masini, A. Bazzi, and A. Zanella, "A survey on the roadmap to mandate on board connectivity and enable V2V-based vehicular sensor networks," *Sensors*, vol. 18, no. 7, p. 2207, 2018.

[16] V. Marojevic, "C-V2X Security Requirements and Procedures: Survey and Research Directions," 2018.

[17] T. Rebbeck, J. Stewart, H.-A. Lacour, A. Lillen, D. McClure, and A. Dunoyer, "Socio-economic benefits of cellular V2X," *Final Report for 5GAA.[(accessed on 31 August 2019)]*, 2017.

[18] R. Freund, T. Haustein, M. Kasparick, K. Mahler, J. Schulz-Zander, L. Thiele, T. Wiegand, and R. Weiler, *5G-Datentransport mit Höchstgeschwindigkeit*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2018, pp. 89–111. [Online]. Available: https://doi.org/10.1007/978-3-662-55890-4_7

[19] E. Dahlman, S. Parkvall, and J. Skold, *5G NR: The next generation wireless access technology*. Academic Press, 2018.

[20] (2020). [Online]. Available: https://www.volkswagen.de/de/modelle-und-konfigurator/der-neue-golf.html#iqdrive

[21] A. Weimerskirch, "V2X security & privacy: the current state and its future," in *ITS World Congress, Orlando, FL*, 2011.

[22] A. Rao, A. Sangwan, A. A. Kherani, A. Varghese, B. Bellur, and R. Shorey, "Secure V2V Communication With Certificate Revocations," in *2007 Mobile Networking for Vehicular Environments*, May 2007, pp. 127–132.

[23] T. Strubbe, N. Thenée, and C. Wieschebrink, "IT-Sicherheit in Kooperativen Intelligenten Verkehrssystemen," *Datenschutz und Datensicherheit - DuD*, vol. 41, no. 4, pp. 223–226, Apr 2017. [Online]. Available: https://doi.org/10.1007/s11623-017-0762-7

[24] B. Brecht and T. Hehn, *A Security Credential Management System for V2X Communications*. Cham: Springer International Publishing, 2019, pp. 83–115. [Online]. Available: https://doi.org/10.1007/978-3-319-94785-3_4

[25] X. Zhang, A. Kunz, and S. Schröder, "Overview of 5G security in 3GPP," in *2017 IEEE Conference on Standards for Communications and Networking (CSCN)*, Sep. 2017, pp. 181–186.

[26] M. S. Anwer and C. Guy, "A survey of VANET technologies," *Journal of Emerging Trends in Computing and Information Sciences*, vol. 5, no. 9, pp. 661–671, 2014.

[27] G. Karagiannis, O. Altintas, E. Ekici, G. Heijenk, B. Jarupan, K. Lin, and T. Weil, "Vehicular Networking: A Survey and Tutorial on Requirements, Architectures, Challenges, Standards and Solutions," *IEEE Communications Surveys Tutorials*, vol. 13, no. 4, pp. 584–616, Fourth 2011.