CELLULAR AND SHORT-RANGE COMMUNICATION: THE BEST OF BOTH WORLDS

Wouter van Haaften / Lydia Meijer / Tom van Engers

PhD. researcher, University of Amsterdam, Leibniz Institute
Nieuwe Achtergracht 166, 1018 WV, Amsterdam, The Netherlands
vanhaaften@uva.nl; http://www.leibnizcenter.org

Senior scientist, TNO, Leibniz Institute
New Babylon, Anna van Buerenplein 1, 2595 DA The Hague, The Netherlands
lydia.meijer@tno.nl; http://www.tno.nl

Professor, University of Amsterdam, TNO, Leibniz Institute
Nieuwe Achtergracht 166, 1018 WV, Amsterdam, The Netherlands
vanengers@uva.nl; http://www.leibnizcenter.org

Keywords: ***GDPR, Delegated Act, C-ITS, IoT, 4G, 5G, WIFI-p (G5)***

Abstract: *The legal provisions of Cooperative Intelligent Transport Systems were planned to enter the next phase, but the EU Council voted down the correspondingly proposed Delegated Act. Amongst others, the exclusively chosen Wifi-p communication technology was not acceptable from a data protection perspective while the telecom sector was shut out to provide data-transmission services for C-ITS. This paper presents an analysis of technologies, including cellular technology, for car-to-car communication within C-ITS, which shows that the data protection flaws in C-ITS can be remedied by using cellular technology instead of Wifi-p, or by allowing encrypted C-ITS messages over Wifi-p and cellular technology to preload the required encryption and decryption keys.*

1. Introduction

Since the roaring twenties of the previous century men have dreamt of self-driving vehicles. In the post-war fifties, the first application on the road to automation appeared in the slipstream of the autopilot used in the aviation sector; the cruise control. Since then multiple steps have been made on the way to the advanced driver-assistance systems (ADAS) that we find on the road today. Most OEMs agree that further relevant automation in ADAS will require a communication system to exchange information on a vehicles position and speed between nearby vehicles. Therefor a communication protocol was developed that would facilitate vehicle to vehicle (V2V) communication to avoid collisions between those vehicles.

To ensure basic uniformity of V2V communication technology and to provide certainty for the automobile industry, a standard had to be established. Beyond increased safety, further benefits of such V2V communications were widely recognized. The industry expects that V2V communication will provide the communication basis that will enable the development of fully automated vehicles and, hence, exclude human error related accidents. The EEEI standard 802.11.p and the derived ITS-G5[1] standard for V2V cooperative communication technology was established in 2010[2]. The first applications of the technology, also known and hereafter referred to as Wifi-p, are cooperative services to improve road safety, the so-called day 1 and day 1.5 services[3]. The Cooperative-Intelligent Transport System (C-ITS) was planned to be the first application of the Wifi-p technology.

1 G5 is not to be confused with the successor of 4G cellular technology: 5G.
2 en.wikipedia.org/wiki/IEEE_802.11p.
3 ec.europa.eu/inea/sites/inea/files/10_its_vandoorne_isabelle_web.pdf p17/18.

However, as we will explain in this article, data protection flaws prevent the deployment of Wifi-p V2V communications in a very fundamental way. The major problem is that via Wifi-p unencrypted messages are broadcasted containing amongst others the MAC-address of the device and location, speed and direction of the vehicle. When received these data could in certain cases be qualified as personal data. So, the vehicle with C-ITS over Wifi-p actually becomes a driving data leak. It is for this reason that the WP29 suggested having a switch on the device with default setting off as a means to give data subjects a certain control over their data. However, because of the contribution to road safety, the communication of C-ITS information is essential. From that point of view C-ITS should not be switched off. This has led to an impasse where C-ITS can neither work with Wifi-p, due to data protection objections, nor without Wifi-p, due to a lack of alternatives.

So, how to get out of this deadlock? In this paper we will point out how cellular technologies like 4G and 5G partially can remedy the flaws in V2V Wifi-p communications. We will show how to combine cellular and Wifi-p technologies in various ways in order to achieve the goals of C-ITS on the one hand and a substantially higher level of compliance with the GDPR on the other hand.

2. V2V Communication technology

The Wifi-p technology that was adapted for the deployment of C-ITS[4] creates a kind of W-Lan around the vehicle. It broadcasts the CAM[5] and DENM[6] messages in a radius of about 500 meters. The choice for this V2V-standard was made in 2012 because of lacking alternatives. When making this choice the reliability of the Wifi-p and its low latency data transfer counted heavily. These capabilities are essential for time critical applications as collision avoidance and other day 1 services. Eventually, so it was expected, the reliability and low latency communications of Wifi-p will enable autonomous vehicles to drive safely. For non-time critical services cellular technology was considered as the alternative[7]. With hindsight, one can state that privacy related aspects of Wifi-p were at first subordinated to low latency capabilities, although data protection had been a point of discussion in the preparation of the IEEE 802.11-p standard.

2.1. Wifi-p and security

The low latency characteristics of Wifi-p required for C-ITS are key in its design. Another requirement is that the CAM messages broadcasted are from a legitimate source, e.g. a certain car. For this reason, authentication certificates are used to establish whether a CAM message key belongs legitimately to a vehicle. The CAM messages broadcasted by the vehicles are signed using a pseudonymized certificate, where an algorithm periodically changes the pseudonym. However, by tracking the car at sufficiently dense intervals a listener to broadcasted CAM messages can relate the vehicles track to a pseudonym and discover when it changes. Such listener could easily discover that between two adjacent positions on the road there was a change in the pseudonym. This means that the executor of a wide-area tracking attack, despite the use of pseudonymized certificates, can follow a car and eventually link the route to driver and/or passenger data.

4 November 2014, the start of the EU C-ITS Platform.
5 Cooperative awareness message.
6 Decentralized environmental notification message.
7 Report EU Platform C-ITS 2016 p. 10.

2.2. Wifi-p and data protection

In its first report[8] it was established by the EU C-ITS Platform on the deployment of C-ITS that the broadcasted CAMs, including MAC[9]-addresses and location of the vehicle may qualify as personal data. That's where the Directive[10], and its successor the GDPR came in. In two previous papers we have analyzed the specific data-protection issues of C-ITS using short range broadcasts[11]. On the request of the EU Commission, assisted by an expert group consisting of stakeholders, the WP29[12] produced an Opinion[13] on the proposed C-ITS and its Wifi-p technology. The WP29 was quite clear about the flaws of Wifi-p regarding data protection within the system. Their most rigorous recommendation was to switch the Wifi-p device off by default. In that case it would always be clear that the choice to be «seen» on the road would be the explicit choice of the driver. Other suggestions of WP29 were to encrypt the messages or at least to lower the frequency of the broadcast and to consider adding noise injection to the signal. This would impede the tracking of the vehicle. It was clear that C-ITS would not be acceptable from a data protection perspective without adjustments to the system.

2.3. Legislative process

In the first drafts of the legislation for C-ITS, the Delegated Act no specific data protection arrangements were included. Only after the Opinion of the WP29 Committee landed in the design process of the Delegated Act, it became clear that the prescription of mandatory use of C-ITS based Wifi-p communication technology was not feasible. The risk that third parties could unlawfully intercept the sequence of messages was simply too high, and the C-ITS concept excluded adequate security measures. So, it was decided that the choice to participate in a relatively unsecure system should be left to the driver of the vehicle. Therefore, an on/off switch was to be implemented in the system in order to give the user the final say in whether he/she wants to participate in C-ITS Wifi-p or not.

In March 2019 the Commission agreed on the final text of the draft Delegated Act and it was adopted by the EU Parliament in April 2019 thus about to become the legal basis for C-ITS. But at that point it already was clear that several OEMs and the telecom sector were not happy with the rigid prescription of Wifi-p. After all, 5G cellular technology was developing rapidly and it was expected to function, due to more efficient use of the available radio spectrum, in situations where Wifi-p would be overloaded like densely populated areas and busy highways. In July 2019 the EU-Council rejected the proposal and the Commission was sent back to the drawing board of C-ITS.

2.4. Hybrid Technology

Since the EU council voted down the Delegated Act, it is clear that changes to the C-ITS concept have become inevitable. One of the major flaws of the envisioned C-ITS technology is the unilateral choice for Wifi-p as the standard for V2V communication. Although the reasons for that choice, low latency and coverage independence, were valid at the time (2008), advancing technology brings new insights as to how C-ITS should

8 Report EU Platform C-ITS 2016.

9 MAC addresses designates the receiver and sender of a Wifi-p transmission. The receiver MAC address is in the case of CAM messages set to indicate all nearby addresses: broadcast address. The sender MAC address is unique for a vehicle and changed regularly to avoid tracking of the vehicle. Tracking a vehicle on basis of an ever randomizing MAC address only, i.e. without its GPS positions is very difficult.

10 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995.

11 W.F. van Haaften/T.M. van Engers, Cooperative Intelligent Transport Systems and the General Data Protection Regulation, Proceedings of the 21st International Legal Informatics Symposium IRIS 2018, W.F. van Haaften/T.M. van Engers, Communication of in-vehicle data and data protection, Proceedings of the 22st International Legal Informatics Symposium IRIS 2019.

12 Working Party Article 29, consisting of the chairs of the EU Data Protection Authorities.

13 Article 29 Data Protection Working Party, Opinion nr 3/2017 on Cooperative-Intelligent Transport Systems, October 2017, http://ec.europa.eu/newsroom/just/document.cfm?docid=47888.

technically be supported. For instance, there are examples that C-ITS can be based solely on cellular communications of CAMs. In the Netherlands, a program called Talking Traffic has already been experimenting successfully with cellular C-ITS used for intelligent traffic light systems. Yet cellular C-ITS cannot beat the very low latency achieved by over-the-air Wifi-p broadcasts which are, in extreme situations, crucial to avoid accidents. Presently, the time seems right for an approach that has been in the air for some time; the hybrid system that combines the cellular and Wifi-p strengths. Regardless of the choice for specific technologies like 3G, 4G or 5G for cellular communication in combination with Wifi-p, the hybrid approach can yield privacy by design[14] qualities. Specifically, as we will show that the unencrypted broadcast of Wifi-p is merely the last resort in the scarce situations where cellular technology is too slow or has no coverage at all.

2.5. Legal framework

So, where do we stand now with short range V2V communication? Apart from the difference in functional characteristics between Wifi-p and cellular technology also from a data protection perspective both technologies have different consequences. First of all, both technologies are ruled by different legislation. Wifi-p, not being a service delivered by a telecom network, is subject to the GDPR[15] while cellular technologies, functioning within a telecom network, are ruled by Directive 2002/58. Although the purpose of both legislations is similar, their differences are relevant. For our purpose the most important issue is that the encrypted communications via the cellular network and the telecom providers is secure and encrypted in alignment with the Directive. That means that from a data protection point of view we do not have to worry about (ab)using cellular communication (see Table 1).

Table 1

	Wifi-P	**Cellular**
Communication prot.	*Broadcast, short range*	*Point to point*,
Transport means	*5.9 band*	*Telecom network*
Data protection	*Authentication certificates*	*Telecom network*
Security	*Not encrypted*	*Encrypted*
Legislation	*GDPR, Reg. 679/2016*	*Directive 2002/58*

In the next paragraphs we will present two ways in which the use of cellular technology can help to increase the data protection compliance of the C-ITS. We discuss two combinations: 1) use the cellular network as much as possible and fall back to Wifi-p combinations if necessary and 2), use cellular telecommunications to preload encryption and decryption keys to adjacent cars to enable secure exchange of CAM over Wifi-p and fall back to Wifi-p combinations if necessary.

2.6. Cellular or Direct V2N

In the combination of cellular and the Wifi-p broadcast the latter could be replaced by a cellular sent CAM. This means that the CAM is not broadcasted directly V2V or V2I, but it is sent to a datacenter via the cellular network, thus solving the mayor data protection flaw, the unencrypted broadcast in the way that the CAM would be sent point to point and would be encrypted. The CAM will be sent to a data center from which the CAM will be sent back immediately to the vehicles and road-side units directly near the vehicle that has send the original CAM. In this way all the vehicles nearby as well as the road authority will be properly informed. The question is, will the CAM be on time? As far as the current state of technology on 4G is concerned the answer would be yes. The transportation of the CAM to and from the datacenter should take between 0.1 and

[14] Article 25 GDPR.

[15] Formerly Directive 95/46/EC.

0.5 seconds maximum, including encryption and decryption. If this latency cannot be realized due to local circumstances, then the unencrypted Wifi-p broadcast could take over.

Although the latter would bring back the data protection objections of lack of security, the mainly cellular operation will cover a substantial part of the data protection concerns. Also, in areas with limited 4G coverage the Wifi-p broadcast could help out. The broadcast of CAMs via Wifi-p would have been reduced to a minimum, thus satisfying the data protection demands to a large extend. In fig. 1 the mixed cellular and direct communication landscape is illustrated in connections 3 and 4. In the next paragraphs we will explain both options for the C-ITS with hybrid technology.

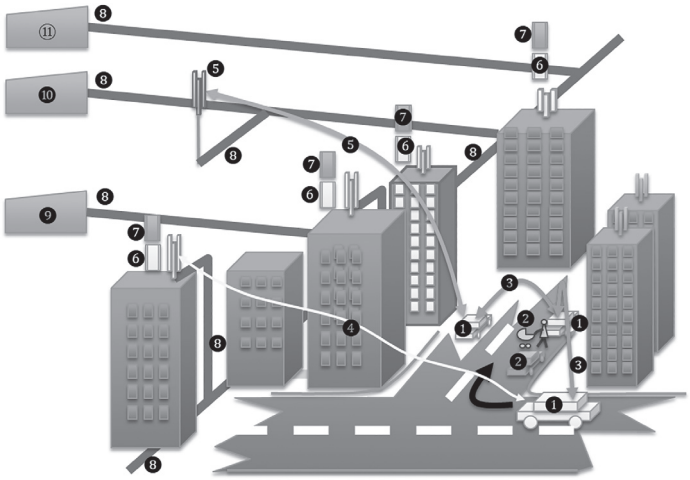

Figure 1 Communications and cloud services for C-ITS

1. Cars running system A, implementation CCAM
2. Other cars, persons, objects
3. G5 link
4. 5G link
5. 4G or any other wireless network link
6. Auxiliary CCAM-software running at 5G edge
7. Any other software running at 5G edge
8. Internet
9. Regional/national data center
10. Data center in EU
11. Data center outside EU

2.7. Wifi-p additional to cellular

In the first option the Wifi-p will be additional to the cellular communication. The starting point would then become to use encrypted cellular communication if possible, and unencrypted Wifi-p communication when inevitable. In this option the CAM of vehicle A (1) is no longer broadcasted but is sent, point to point, to the data center (9) via secure cellular communications (4). The data center sends the CAM back to vehicles near vehicle A via the same secure cellular communication technology (4). The other vehicles (1), and e.g. C-ITS roadside stations, receive the secured CAM via the cellular network. The critical test for this procedure in the first instance of C-ITS is whether this process can be completed fast enough to facilitate day 1 and day

1.5 services. If this is not the case, or if no cellular coverage is available at all, the conventional method of unencrypted CAMs being broadcasted will function as the fall back option.

2.8. Cellular supporting Wifi-p

In the second option this data protection flaw of the transmission of C-ITS CAM messages over Wifi-p is overcome to a large extend by combining the technologies in a way that feels a bit like the application of diesel engines in trains, where the diesel power is used to activate the electric traction. The combination should include a datacenter and cellular (4G/5G) communication to and from the vehicles. The cellular communication could preload encryption keys to the vehicle, only usable along a limited section of the road and a limited amount of time. This would lead to a new approach of C-ITS: cellularly supported encryption of the full contents of the CAM broadcast when available and safe, unencrypted CAM broadcast as a fall back scenario in case no cellular connection is available, or the response time is too long for safe operation in traffic.

In Fig. 1 this will be represented as follows: The vehicle A (1) reports itself to the data center (9) via secure cellular communication (4). The data center sends back to vehicle A an encryption key (4). At the same time the data center sends a corresponding decryption key to vehicles known to be in the neighborhood of vehicle A (4). Then vehicle A broadcasts its encrypted CAM (3). The other vehicles (1), and e.g. C-ITS road-side units, receive the CAM, decrypt it and process it as they would have in the unencrypted C-ITS variant. Also, in this case the critical test would be whether this process can be completed fast enough to facilitate day 1 and day 1.5 services. One could expect so, since only the keys for (very near) future CAMs have to be sent and received. However, if the latency is too high, or if no cellular coverage is available at all, the conventional method of unencrypted CAMs being broadcasted will be the fall back option.

Table 2 The various situations and consequences illustrated

Situation	***4G CAM***	***5G CAM***	***G5***	***4G Encryption keys***	**5G *Encryption keys***	***G5***
V (Vehicle) alone	①②			①②		
Vs nearing another	①②③			①②③		③④
Vs separating	⑥⑦			⑥		⑦
Failure Internet/4G			⑤		⑧⑨⑩	④
Failure 4G/5G			⑤			⑤
Failure G5	①②③	①②③		①②③	①②③	

Normal situation, cellular available
① CAM of V reported to datacenter ❾
② CAM of nearby Vs securely reported from ❾ to V
③ CAM of V and nearby Vs securely exchanged via ❾ and via ❺ including de- and encryption keys
④ encrypted CAM(s) broadcasted over Wifi-p

In case no cellular coverage or enough time;
⑤ unencrypted CAM broadcasted
⑥ all info deleted from ❾
⑦ all info deleted from Vs
Fall back on 5G (unlikely)
⑧ 5G-authorisation
⑨ public-key exchange system setup ❻ at 5G-edge
⑩ other (local) services ❼ at 5G-edge.

2.9. System adaption

What would this mean for the C-ITS as foreseen at the moment? For the chosen Wifi-p standardization of C-ITS it would not mean much in terms of basic technology. The device broadcasting the CAM should still be in the vehicle and available for use. One could decide to choose another, perhaps more up-to-date, standard, but the principle of broadcasting short range CAMs would remain unchanged. In variant 1, where telecommunication takes over when available, the default setting would be «off», and the setting «on» would have to be activated depending on availability and usability of the primary telecommunication system. In variant 2, the support of Wifi-p by preloading en- and decryption keys, the possibility of sending encrypted messages would have to be added to the C-ITS devices. For both variants a cellular interface should have to be added to the C-ITS device. Table 2 shows the operational consequences.

2.10. Long term perspective

Up to now the perspective of the Delegated Act and of the EU efforts to establish an acceptable system for day 1 and day 1.5 services with C-ITS Wifi-p is not exactly glorious. But what about the future V2V communication between autonomous vehicles? Chances are that Wifi-p, or any other short-range broadcasting service, will still appear to be the fastest and most adequate way to inform other vehicles. This V2V communication could be crucial to this very time critical application. Perhaps one would not use encryption to save time. What would be the consequences from a data protection point of view? Given the fact that the vehicles will have no driver the concern of data protection will decrease. However, it will not disappear, since data protection should also be guaranteed for the passengers in the vehicle when broadcasting data. It is not to be foreseen that autonomous/cooperative vehicles will be out of the realm of data protection law altogether, but if 5G would be able to replace Wifi-p or similar technologies with the same low latency and reliability it would be a lot easier to comply with data protection law.

2.11. Legal issues

In this paragraph we will look into the specific legal data protection issues related to both the proposed alternatives for C-ITS Wifi-p, starting with the description of the relevant distinctions and similarities between them. First of all, it is good to realize that the original model, in which the CAMs are unencrypted short-range broadcasted, will still be the fall back scenario. This means that the data protection flaws as signaled by the WP29 will not entirely disappear. However, they will be reduced to specific circumstances, like the absence of cellular coverage or too much latency in the cellular network. In our opinion that also means that the ultimate data protection tool, the on/off switch, could be taken off. After all, the number of occasions on which the CAMs will be broadcasted unencrypted will be very limited.

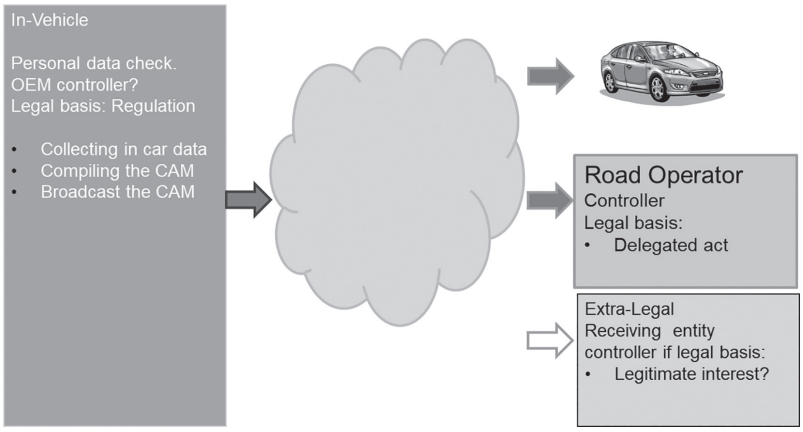

Figure 2 Full Wifi-p unencrypted short-range broadcast

2.12. CAMs over cellular

In the first option the CAM will be sent directly to a datacenter, and then sent back to the vehicles in the neighborhood of the sending vehicle. This communication will run via the cellular network. From a data protection perspective this means that the Directive 2002/58 will be applicable. This Directive for telecom networks legally protects the data that is being transported over telecom networks more or less in the same way that paper letters in envelopes are protected. The telecom provider has no admission to the content of the message, i.e. the CAM. It merely transports the message from the sender to the receiver, or provides for a, confidential[16], telecom line. The traffic that is being transported over the telecom lines will be encrypted in order to shield the content[17].

The data center that receives the CAMs and sends them back to the neighboring vehicles will also be subject to data protection regulations, either as a provider of value-added services within the scope of the Directive, or as a C-ITS service provider under the GDPR regime. As far as the legal basis and other conditions are concerned, they are out of scope of this paper in which we concentrate on the specific differences between short-range and cellular communications.

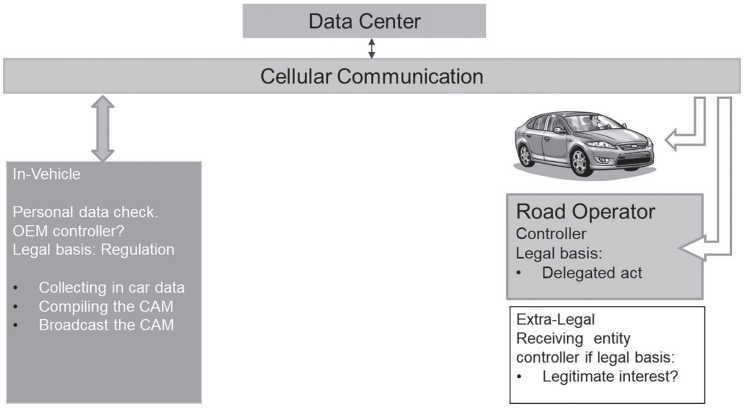

Figure 3 Full telecom C-ITS system, unencrypted broadcast (Fig 1) as fall back

[16] Article 5 of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002.
[17] Article 4 of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002.

In this option all CAMs from the vehicle and to other vehicles are being sent via cellular connections. From the car to the data center, and back to several cars and to the road-side unit in the direct environment of the sending vehicle. As long as sufficient coverage and low latency will be available this option can work within the telecom data protection realm. All communication is point to point encrypted and cannot be approached by third parties. The position of the data center will need to be established due to its public task to provide for CAM messages. In principle the system could function with 3G capabilities or higher standards e.g. 4G and 5G. In case no cellular network is available or when the network cannot provide the service level required the system will switch to the fall back option: the unencrypted broadcast as shown in fig. 2.[18]

2.13. Keys over cellular

Another, more advanced and future-proof use of hybrid technology could be to broadcast short-range, and to use the cellular environment, 3G or higher, to provide the vehicles with encryption and decryption keys. In that case a vehicle pushes its CAM to a data center that in response delivers an encryption key to the car and simultaneously decryption keys to nearby vehicles and road-side-units. The vehicle then will send encrypted CAMs that can be unencrypted by the nearby vehicles and road-side-units. The advantage will be that the sending of the keys can be done in advance as the data center can track the movements of the vehicles. Pre-loaded with keys in this way the low latency CAM broadcast will be maintained regardless of the cellular signal or coverage. Only if the vehicles have not received decryption keys, or when the key handling takes too long, the system will switch over to the fall back; the unencrypted short-range broadcast.

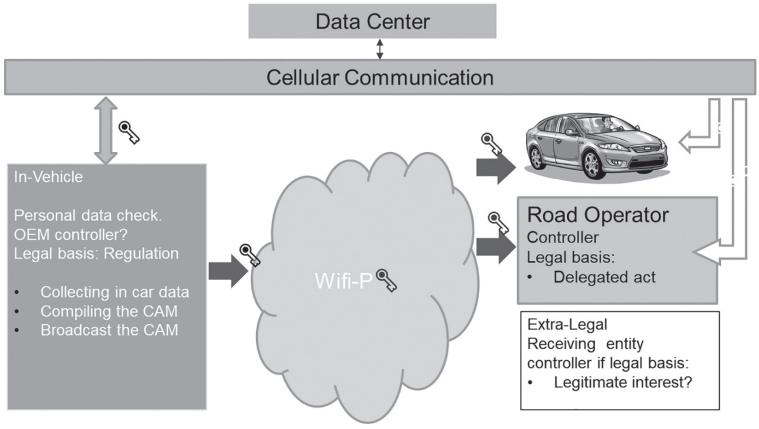

Fig.4 Encrypted broadcast supported by cellular provided en- decryption keys. Fall back: unencrypted broadcast.

The figure shows the original short-range broadcast supported by independent encryption key traffic via cellular connections. The role of the data center/service, the provider of the encryption and decryption keys, will have to be regulated. The use of cellular technology in this way is much more dedicated to the system than the role in the variant where CAM messages are sent directly to the vehicles.

From a data protection and road safety perspective this solution offers the best of both worlds. Low latency direct communication V2V and V2I, supported by less time critical supply of encryption and decryption keys

[18] W.F. van Haaften/T.M. van Engers, Communication of in-vehicle data and data protection, Proceedings of the 22st International Legal Informatics Symposium IRIS 2019.

via cellular communication. A specific point of attention is that the encryption method should not take so much time that it jeopardizes the required very low latency of the V2V broadcast.

3. Conclusions

In this paper we have demonstrated that there are at least two alternative options in which cellular technology can help to overcome the fatal data protection flaws of Wifi-p as the selected technology for C-ITS. The first one is effectively used in the Dutch pilots with intelligent traffic light systems[19]. It can be a relatively simple and fast way of getting started with the deployment of C-ITS since the cellular communication is already standardized to a high extend. An advantage could be that the Wifi-p standard itself would possibly not have to be adapted. The downside is that it remains to be seen whether the latency is low, and the coverage will be dense enough to be able to cover the needs of the day 1 and day 1.5 services. Eventually this option may only work for the M2M communication of autonomous vehicles, when a Wifi-p back-up system will be added.

The second option, providing encrypted broadcasting of CAM messages seems the more future-proof solution. Except for situations where over a longer amount of time no cellular support will be available, this technology will support secure C-ITS over Wifi-p in most circumstances. It can therefore effectively decrease the amount of unencrypted CAM messages to a very low level, thus meeting the concerns of the WP29 data protection Authorities to a large extend. It will take away most reasons for the data protection risks, as perceived by the WP29, like disclosure of the driving position of the vehicle, lack of transparency as vehicles broadcast continuously and data leakage.

Furthermore, it provides for a full partnership of the telecom sector in C-ITS. In fact, although the standards remain the same, option two would make C-ITS a much more technology-independent proposition. Our conclusion is that the combination of Wifi-p and cellular C-ITS does no longer create insurmountable data protection liabilities.

3.1. Acknowledgements

The research for this paper is a part of the RAAK Pro financed VIA NOVA project developing a generic measure in which the specific quality of the data from cars and needed quantity is related to the potential use of the data, using the principles of Big Data analysis. Privacy and security issues with respect to data from cars play a central role in defining the usability of the data and are therefore addressed in VIA NOVA.

The authors thank the European Commission for the opportunity to contribute to Working Group 5 – Cybersecurity and access to in-vehicle data linked to CCAM of the Simpcamp[20] project (2019).

References:

European Parliament and of the Council Regulation 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) OJEU L119, 4 May 2016.

European Parliament and of the Council Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJEC L281/31, 24 October 2002,

European Parliament and of the Council Directive 2002/58/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJEC L201/37, 12 July 2002,

[19] Within the framework of the Talking Traffic program. In this application no Wifi-p backup system is foreseen.

[20] SIMPCAMP: Support for the Implementation of the single Platform for open road testing and pre-deployment of Cooperative, connected Automated and autonomous Mobility Platform.

Article 29 Data Protection Working Party, Opinion nr 3/2017 on Cooperative-Intelligent Transport Systems, October 2017, http://ec.europa.eu/newsroom/just/document.cfm?docid=47888

Cooperative Intelligent Transport Systems Platform C-ITS), Final Report Data Protection & Privacy Analysis of Data Protection & Privacy in the context of C-ITS, Recommendations and guidelines, Based on the work of WG-4 of the C-ITS Platform Annex to Final Report Version 1.2 – January 2016, https://ec.europa.eu/transport/sites/transport/files/themes/its/road/actionplan/doc/c-its-platform/2016annexestothec-itsplatformfinalreportjanuary2016.zip

European Standard ETSI EN 302 637-2 on Intelligent Transport System V1.3.0. 2013-8 ITS vehicle comm. Specs. Cooperative awareness service, August 2013, https://www.etsi.org/deliver/etsien/302600302699/30263702/01.03.0130/en30263702v010301v.pdf

European Standard ETSI EN 102 638 on Intelligent Transport Systems V1.1.1. 2009-6 ITS Vehicle comm. Basic set application definition, June 2009, https://www.etsi.org/deliver/etsitr/102600102699/102638/01.01.0160/tr102638v010101p.pdf

W. van Haaften & J. Wennekers & T. van Engers, Data Protection and C-ITS – A Use Case, Proceedings of the 11th EU ITS Conference, Glasgow. W. van Haaften & T. van Engers, Data Protection and C-ITS – Personal Data, 12th EU ITS Conference, Strasbourg.

Gemeinsame Erklärung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder und des Verbandes der Automobilindustrie (VDA), Berlin, 26 January 2016.

W.F. van Haaften/T.M. van Engers, Cooperative Intelligent Transport Systems and the General Data Protection Regulation, Proceedings of the 21st International Legal Informatics Symposium IRIS 2018

W.F. van Haaften/T.M. van Engers, Data Protection and C-ITS, a personal data proposition Proceedings of the Amsterdam Privacy Conference 2018.

W.F. van Haaften/T.M. van Engers, Communication of in-vehicle data and data protection, Proceedings of the 22st International Legal Informatics Symposium IRIS 2019.

https://en.wikipedia.org/wiki/IEEE_802.11p (12 December 2019)

https://ec.europa.eu/inea/sites/inea/files/10_its_vandoorne_isabelle_web.pdf p17/18 (12 December 2019)