Misuse Capabilities of the V2V Communication to Harm the Privacy of Vehicles and Drivers

Markus Ullmann,* † Thomas Strubbe,* and Christian Wieschebrink*
* Federal Office for Information Security
D-53133 Bonn, Germany
Email: {markus.ullmann, thomas.strubbe, christian.wieschebrink}@bsi.bund.de
† University of Applied Sciences Bonn-Rhine-Sieg
Institute for Security Research
D-53757 Sankt Augustin, Germany
Email: markus.ullmann@h-brs.de

***Abstract*—A deployment of the Vehicle-2-Vehicle communication technology according to ETSI is in preparation in Europe. Currently, a policy for a necessary Public Key Infrastructure to enrol cryptographic keys and certificates for vehicles and infrastructure component is in discussion to enable an interoperable Vehicle-2-Vehicle communication. Vehicle-2-Vehicle communication means that vehicles periodically send Cooperative Awareness Messages. These messages contain the current geographic position, driving direction, speed, acceleration, and the current time of a vehicle. To protect privacy (location privacy, "speed privacy") of vehicles and drivers ETSI provides a specific pseudonym concept. We show that the Vehicle-2-Vehicle communication can be misused by an attacker to plot a trace of sequent Cooperative Awareness Messages and to link this trace to a specific vehicle. Such a trace is non-disputable due to the cryptographic signing of the messages. So, the periodically sending of Cooperative Awareness Messages causes privacy problems even if the pseudonym concept is applied.**

***Keywords*–Vehicular Ad hoc Networks; Vehicle-2-Vehicle Communication; Intelligent Transport System; Cooperative Awareness Message; Pseudonym Concept; Privacy**

I. INTRODUCTION

A first brief analysis of the mentioned privacy problems caused by Cooperative Awareness Messages is given in [1] and [2]. The vehicle-to-vehicle (V2V) and vehicle-to-infrastructure communication (V2I) (consolidated V2X) have been intensively discussed in recent years. The deployment of this technology requires accepted standards. The neccessary specification and standardization in Europe is done by the European Telecommunications Standards Institute (ETSI) based on considerations of the Car2Car Communication Consortium [3]. This includes the security standardization as well [4].

The ETSI specifications define an architecture for Intelligent Transport Systems (ITS). This architecture specifies different ITS stations (e.g., ITS roadside stations, and ITS vehicle stations) and wireless communication between the ITS stations. The wireless communication technology for cooperative V2X communication is based on the IEEE 802.11p standard. A frequency spectrum in the 5.9 GHz range has been allocated on a harmonized basis in Europe in line with similar allocations in US.

The ETSI communication model defines broadcast communication between ITS stations. Different message types are specified for information exchange. These are the Cooperative Awareness Message (CAM) and the Decentralized Environmental Notification Message (DENM). These messages are disseminated via broadcast. According the ETSI specifications CAMs and DENMs shall be digitally signed by the sender (ITS vehicle station or ITS roadside station) to guarantee message integrity and authenticity. In order to issue and authenticate the corresponding cryptographic keys, a suitable public key infrastructure (PKI) has to be established.

At the moment, the deployment of V2X technology is in preparation in large scale intelligent mobility infrastructure projects, for example SCOOP@F [5] in France, the C-ITS corridor Rotterdam-Frankfurt-Vienna [6], and the Nordic Way [7], a joint project of Denmark, Finland, Norway, and Sweden. In the meantime, the European Commission published a strategy "Towards Cooperative, Connected and Automated Mobility" which announce the deployment of the V2V communication in Europe beginning 2019 [8].

Each ITS vehicle station leaves a signed trace of its geographic location. Each entity within the communication range of the ITS communication technology can receive that data. In the final report of the C-ITS platform (January 2016) of the EC DG MOVE the data elements of CAMs and DENMs of ITS vehicle stations are rated as *personal data* [9].

In this paper, we show that it is possible to link sequent CAMs of a vehicle to a CAM-trace even in case of a pseudonym switch. A side effect of cryptographic signed CAMs is that the transmission of the CAM data is not disputable. The applied cryptographic ECC domain parameters (NIST P-256 [10], BrainpoolP-256r1 [11]) are such that ECDSA signatures are not manipulable within the next years. We show in Section V-B, that an attacker can misuse the existing V2V communication to plot a CAM-trace of a vehicle. If only one CAM of the whole trace can be linked to a specific vehicle then the whole trace can be linked to this vehicle. So, CAMs provide side effects which can totally jeopardize the privacy of motorist. The privacy shortcomings of the CAMs are raised by the combination of following issues:

- the amount of included data within CAMs,
- the cryptographic signing of CAMs with distinct pseudonymous keys (non-disputable property),
- the CAM frequency of up to 10 Hz,

- the linkability of CAMs to traces of specific vehicles, and
- the linkage of non-disputable CAM-traces to a specific vehicle.

Modern vehicles are equipped with wireless interfaces, like Bluetooth, to connect devices (smart phones, tablets, etc.) to the multimedia component (head-unit) of the vehicle. Furthermore, head-units are increasingly able to establish Wi-Fi hotspots to support internet access for vehicle passengers. These wireless interfaces have nothing to do with the V2V communication. But from an attacker perspective these interfaces enable to link captured CAM-traces to a specific vehicle. Therefore, these wireless vehicular interfaces have to be regarded in a holistic security analysis of the V2V technology as well.

The following sections of this paper are organized as follows: Section II is a description of related work. Next, Section III provides a brief overview of the secure V2V communication specified in the ETSI standards. Especially, the suggested pseudonym concept for securing CAM and DENM messages is presented in detail. One important privacy requirement of the V2V communication is that CAMs can not be linked over a longer time period. But in Section IV is shown how CAMs of a vehicle can be technically linked to a CAM-trace of a vehicle. How vehicles can be monitored in a non-disputable manner based on an observation device is presented in Section V. Next, an analysis of the captured information is given in Section VI. Finally, in Section VII we summarize our results, mention open research issues and propose requirements for a future V2V communication technology. Subsequent, identifiers for ITS vehicle stations are presented in Section B.

II. Related Work

A detailed overview of attacks in vehicular ad-hoc networks (VANETs) is given by Ghassan Samara et al. [12]. A security and privacy architecture for pseudonymous message signing is described by Papadimitratos et al. [13]. Julien Freudiger et al. suggested mix zones for location privacy in vehicular networks [14]. A survey on pseudonym schemes in vehicular networks is given by Petit et al. [15].

Wiedersheim et al. [16] analyzed the location privacy in a specific communication scenario. Vehicles periodically send beacon messages. The beacons only carry the geographic position and an identifier. To support location privacy, the vehicles use pseudonymous identifier, which are changed regularly. Assuming a passive attacker who is able to eavesdrop the communication in a specific region. Then the attacker is able to track the vehicles with an accuracy of almost 100% if he uses the approach in [16]. To perform this attack in a larger area an infrastructure of receivers is necessary to collect the CAM data. This can be done, e.g., by

- ITS roadside stations or
- an ITS vehicle fleet (e.g., truck fleet)

Besides the identification of ITS vehicle stations based on licence plates or cryptographic certificates the identification based on noise features (individual noise spectrum) are discussed. That is a very active research area and different studies are presented [17] [18]. They differ in concerning single or multi sensor usage and concrete feature extraction. Surprisingly, neither common security nor privacy analysis of the V2V communication consider this issue. Also, Bluetooth MAC IDs of vehicular multi-media devices are already used to develop route specific origin-destination tables and to perform traffic counting on specific roads. Carpenter et al. [19] performed an analysis in Jacksonville, Florida. Therefore, a set of Bluetooth receivers was located at the roadside on specific streets to capture the Bluetooth MAC ID of crossing vehicles. The identification and tracking of vehicles based on Secondary Vehicle Identifier (e.g., Bluetooth interfaces, Wi-Fi hotspots, ...) is presented in [20].

Further identification techniques allow wireless devices to be identified by unique characteristics of their analog (radio) circuitry; this type of identification is also referred to as physical-layer device identification. Physical-layer device identification is possible due to hardware imperfections in the analog circuitry of transmitter introduced at the manufacturing process. An good overview concerning the physical fingerprinting of different wireless communication technologies is given in [21]. Especially IEEE 802.11a compliant transmitters are investigated in [22]. Baldini et al. analyzed physical-layer device identification of IEEE 802.11p compliant transmitter based on statistical features [23].

III. Secure V2X Communication

In Europe and US, V2X broadcast communication is provided based on IEEE 802.11p. IEEE 802.11p is a dedicated short-range communication (DSRC) technology with a communication range of up to 800 m in open space. 75 MHz of the DSRC spectrum at 5.9 GHz are exclusively used for the V2X communication. The overall bandwidth is divided into seven frequency channels. IEEE 802.11p is technologically very similar to IEEE 802.11a or IEEE 802.11g. The IEEE 802.11 family provides frequency channels of 5 MHz, 10 MHz, and 20 MHz. IEEE 802.11a uses the full clocked mode with 20 MHz bandwidth while IEEE 802.11p uses the half clocked mode with 10 MHz bandwidth. 5 MHz, and 10 MHz bandwidth can be achieved by using a reduced clock rate. Due to the half clock mode of IEEE 802.11p, in contrast to IEEE 802.11a, the guard time is doppled from 0,8 μs to 1,6 μs [24], [25], and [26].

A. V2V Communication according to the European Telecommunication Standards (ETSI)

The ETSI specification [27] defines a basic set of applications for ITS, like active road safety (e.g., emergency vehicle warning), co-operative traffic efficiency (e.g., regular speed), co-operative local services (e.g., automatic access control), and global internet services (e.g., fleet management).

The ETSI ITS architecture [27] distinguishes 4 different ITS station types: ITS roadside stations (typically termed road side unit), ITS vehicle stations, ITS central stations (e.g., traffic operator or service provider), and ITS personal stations (e.g., a handheld device of a cyclist or pedestrian such as a smart phone).

The ITS stations exchange information based on two different specified message types: CAMs, and DENMs.

To fulfill the security- and privacy requirements, ITS stations will be equipped with two classes of key pairs/certificates based on elliptic curve cryptography (ECC):

1) Long term key pairs (certificates termed enrollment credentials by ETSI) and
2) Pseudonymous key pairs (certificates termed authorization tickets by ETSI)

Due to privacy reasons authorization tickets may not be linked in any way to enrollment credentials or any other vehicle identifier.

The following privacy requirements have to be fulfilled by the V2V communication to guarantee the privacy (e.g., location privacy) of motorists:

1) Pseudonymity of the sender identity and
2) Unlinkability of CAMs to CAM-traces of vehicles over longer time periods

Based on the long term key pair an ITS vehicle station is able to authenticate itself, e.g., against a certification authority (Pseudonym Certification Authority termed Authorization Authority according to ETSI). Cryptographic keys and corresponding pseudonymous certificates (termed authorization tickets by ETSI) are used to secure the CAMs and DENMs mentioned below. It is assumed that pseudonymous certificates are not directly linkable to the identity of an ITS vehicle station.

1) Cooperative Awareness Message: Cooperative Awareness Messages are comparable to beacon messages. They are broadcasted periodically with a packet generation rate of 1 up to 10 Hz. Based on received CAM messages, ITS vehicle stations can calculate a local dynamic traffic map of their environment. A CAM reveals a lot of dynamic information about the associated ITS vehicle station: geographic position, speed, driving direction, etc., at a specific time. In addition, static information, e.g., the length and width (stated with a precision of 10 centimeters) of the ITS vehicle station and the confidence levels of heading, speed, acceleration, curvature and yaw rate are given.

To assure message integrity and authenticity CAMs contain an electronic signature and the appropriate certificate (as signature algorithm ECDSA, which operates on elliptic curves, is used). Then the receiver is able to cryptographically verify the message and check the temporal validity (temporary freshness). It is not planned to forward CAMs hop-by-hop. Figure 1 illustrates the structure of a CAM, which is specified in detail in [28].

Regarding ECDSA based on NIST P-256 a CAM without special container has a size of about 2 kbit. These 2 kbit are splitted into 200 bits for coding the basic -, high frequency - and low frequency container, 750 bits for the header and the ECDSA signature and nearly 1 kbit for a certificate according to the ETSI format [4]. So, only about 10 % of the whole CAM message size is used for the data elements. The remainder 1,8 kbit are necessary for coding the CAM header, the ECDSA signature and the certificate of the appropriate public key.

2) Decentralized Environmental Notification Message: In contrast, the second message type, Decentralized Environmental Notification Message, is event-driven and indicate a specific safety situation, e.g., road works warnings (from an ITS roadside station) or a damaged vehicle warnings (from an ITS vehicle station). The DENM message format is specified in detail in [29]. DENMs can be transmitted hop-by-hop. Figure 2 illustrates the structure of a Decentralized Environmental Notification Message.

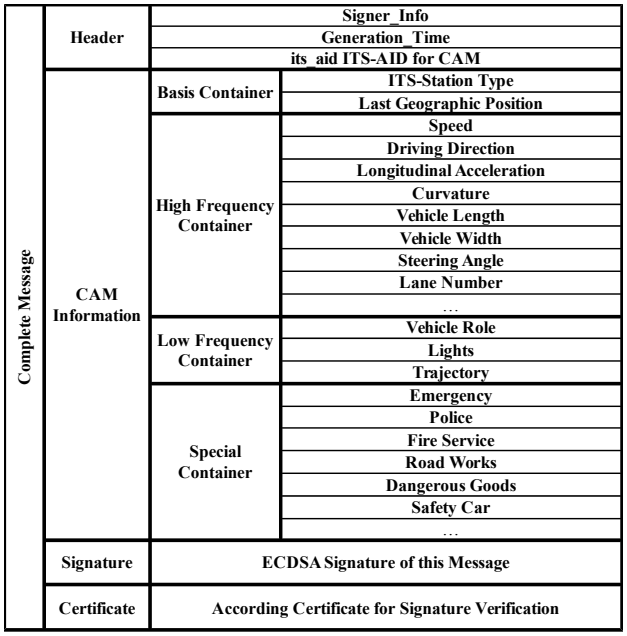


Figure 1. Examplary message format of a CAM. The CAM consists of a header, different data containers, e.g., the basis container, a signature and the appropriate certificate

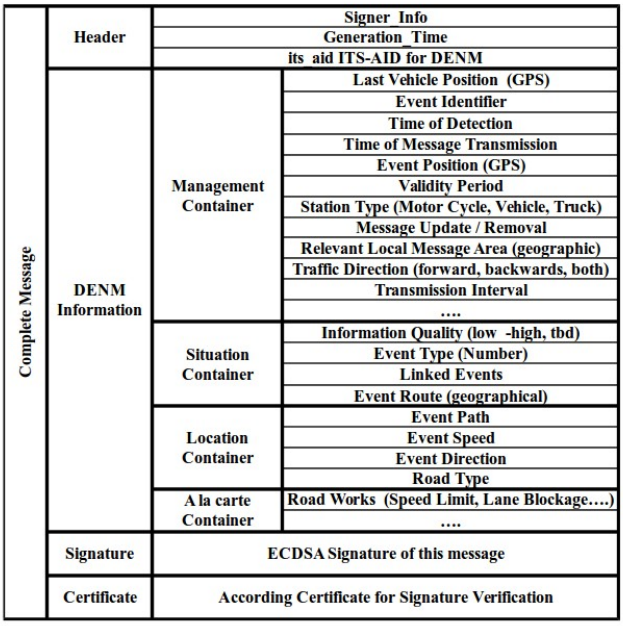


Figure 2. Examplary message format of a DENM. The DENM consists of a header, different data containers, e.g., the management container, a signature and the appropriate certificate.

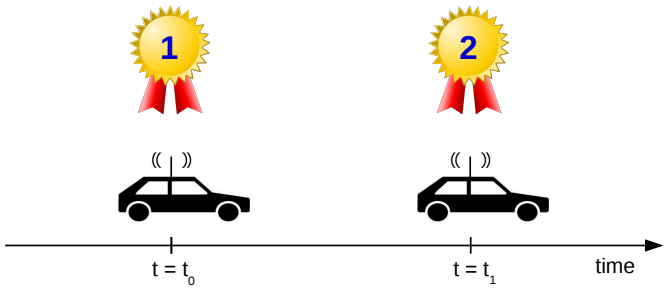
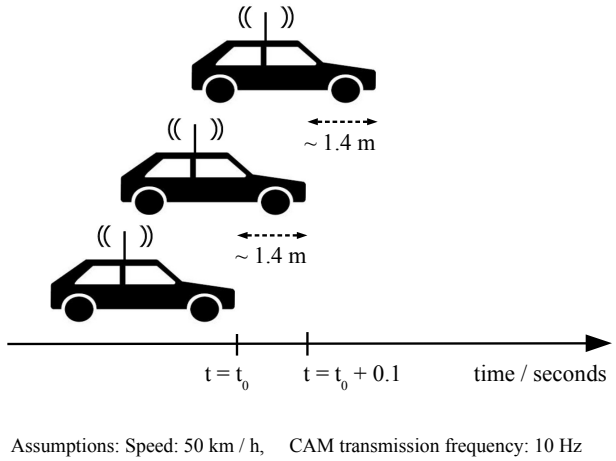


Figure 3. Pseudonymous key switch for signing CAMs respective DENMs (pseudonym concept). Till time point t_0 pseudonym "1" is used for signing the CAM. At time point t_1 a key switch to pseudonym "2" is performed.



Assumptions: Speed: 50 km / h, CAM transmission frequency: 10 Hz

Figure 4. Movement of an ITS vehicle station within 100 ms based on a speed of 50 km/h

3) Pseudonymous Signatures: CAMs and DENMs should not reveal the identity of ITS vehicle stations (sender anonymity). Furthermore, it should not be possible to link messages of an ITS vehicle station (message unlinkability) over longer time periods. Both requirements shall be sufficient to assure location privacy of the ITS vehicle stations. Due to these privacy requirements, CAMs and DENMs are signed using pseudonymous ECC keys, which are not publicly linked to a vehicle. The pseudonymous ECC keys are randomly chosen. Keys used for signing and their appropriate certificates are periodically changed during operation. Therefore, an ITS vehicle station needs a set of pseudonymous keys and certificates valid for some period of time. Figure 3 depicts the usage of the pseudonyms. At time point t_0 pseudonym "1" is still used for signing the CAM. Then the used pseudonym is switched to pseudonym "2". So, in contrast to time point t_0 at time point t_1 pseudonym "2" is used for signing during the next time frame.

Moreover, the applied elliptic curve domain parameters (NIST P-256 or BrainpoolP-256r1) are such that ECDSA signatures are not manipulable within the next years. Therefore, the effect of cryptographic signing of data is that the transmission of this data is non-disputable.

IV. Linkability of V2V Messages

Each CAM includes a pseudonymous certificate. The according secret key is used to sign the CAMs for a short time frame, e.g., 15 minutes. As long as the same key for signing is used the according certificate is static. So, this static information at the end of each CAM can be easily used to link sequent CAMs of an ITS vehicle station. The pseudonym concept (change keys during operation) is applied to prohibit the linkability of CAMs after a pseudonym switch. But a linkability of CAMs is even possible based on the (static) CAM data elements shown next.

A. Linkability of CAMs based on Data

First, static CAM data elements (e.g., vehicle length and vehicle width, and the confidence level of heading, speed, acceleration, curvature and yaw rate) are helpful to link CAMs. Furthermore, the trajectory (included in the low frequency container of the CAM) can be used, too.

Besides that, some information only change very slightly within a time frame of 100 ms: The speed and the geographic position and can be used as well.

The requested transmission rate for CAMs are up to 10 messages each second. Figure 4 illustrates that an ITS vehicle station moves on nearly 1.4 m in this case if the speed is 50 km/h. 50 km/h is the permitted speed in towns in Europe. Assuming that an ITS vehicle station has a minimum length of 3 m: So the geographic position of the length of an ITS vehicle station overlaps at least 50 %. If the ITS vehicle station is longer than 3 m it overlaps much more than 50 %. So, no other ITS vehicle station can physically be at the same geographic position. In addition, linkability of subsequent CAMs of a specific ITS vehicle station is constituted based on the geographic position included in CAMs. Next, the linkability of CAMs is exploited to plot complete CAM traces of drives of a specific vehicle.

V. Observing a Specific Vehicle including the Driver

Wiedersheim et al. [16] analyzed the location privacy of vehicles in a specific area based on a set of distributed receivers.

In contrast to Wiedersheim et al., we show that it is very easy to monitor specific vehicles (driver) in a way that the plotted data (time, location, speed, ...) is non-disputable. The specific *non-disputable property* comes along with the cryptographic signing (ECDSA signature) of the CAM data elements, described in Section III-A3.

But, a specific observation device is necessary to perform our attack, see Figure 5.

A. Observation Device

The basic idea is to stick an electronic observation device at the ITS vehicle station under surveillance. In the ETSI

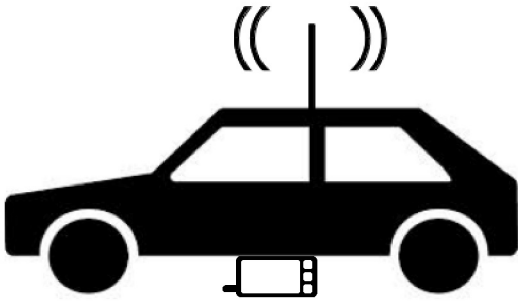


Figure 5. The V2V communication can be missued to monitor a specific vehicle. Therefore, an observation device (e.g., smart phone) has to be invisible sticked at the vehicle under surveillance.

specification it is provided that ITS personal stations (e.g., a handheld device of a cyclist such as a smart phone) take part in the communication. So, if V2V communication components will be broadly deployed we expect that smart phones will support communication according IEEE 802.11p in the 5,9 GHz frequency band in future, too. This is why we exemplarily choose a smart phone as *observation device*. In addition, further components (e.g., GPS receiver) and sensor elements (e.g., accelerometer, gyroscope and magnetometer) are integrated in a smart phone which can also be used for monitoring purposes. But our observation device is not limited to smart phones. Any V2V communication component can be used as observation device.

B. Performing the Attack

1) Capture a CAM-Trace of a Vehicle: After sticking the observation device at a specific vehicle the observation device knows the GPS position of the vehicle based on its internal GPS measurement. So, it can easily exfiltrate CAMs which are sent from external devices at the start time of a vehicular drive. Subsequently, CAMs have to be parsed concerning the included data elements: time, geographic position, certificate as well as the static information: length, width, and the confidence level of heading, speed, acceleration, curvature and yaw rate. These information are sufficient to link and store successive CAMs, as mentioned in Section IV. CAMs which are sent from an outer geographic position can be exfiltrated and discarded. If a whole drive is monitored with our observation device, then a continous CAM-trace (from starting point to the destination) of the ITS vehicle station exists. If the observation device is sticked at the ITS vehicle device over a longer period, a couple of drives can be monitored. Only the really battery power and the available memory (one CAM has a size of about 2 Kbit) of the observation device will be the limiting factors. The different CAMs of a drive can be linked based on the submission time and the static pseudonym certificate. Due to the linkage of data even a pseudonym switch does not interrupt the linkage of sequentiall CAMs as shown before. So, with this kind of observation device it is possible to capture CAM-traces of complete drives of a vehicle. Also it is possible, that CAMs, received by the observation device, are directly communicated to a control and command center, e.g., via the LTE interface.

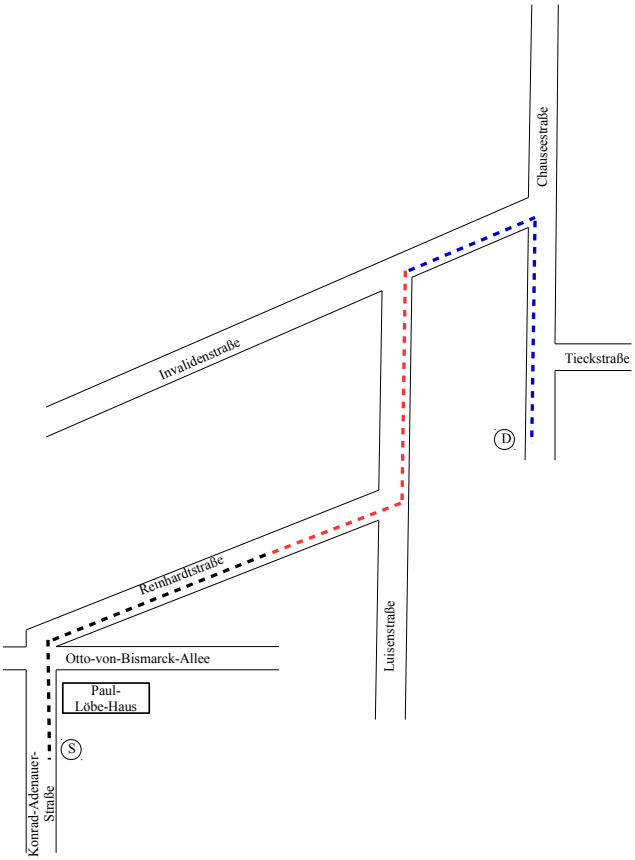


Figure 6. Examplary geographic position of a captured CAM-trace of a personal driven vehicle in Berlin. The colored dotted lines indicate pseudonymously signed CAMs of one specific vehicle. Here, three different pseudonyms (“black” line, “red” line, and “blue” line) are used during the drive

Figure 6 shows a vehicular drive beginning at the start position “S” and finishes the drive at the destination “D”. Next, we are interested to link captured CAM traces to a specific vehicle or driver based on additionally captured information of the vehicle.

Quite the same CAM trace can be captured if an attacker actively follows the vehicle under observation and stores the received CAMs as CAM trace.

2) Capture Secondary Vehicular Identifier: Secondary Vehicle Identifier (Appendix B-B) were analyzed in detail in [30]. Moreover, measurements with available tools for smart phones and PCs were performed. This measurements show, that Bluetooth MAC IDs of active vehicle Bluetooth interfaces of vehicular head-units are easily detectable. E.g., the Bluetooth MAC ID of the head-unit of a standstill Skoda Octavia III could be detected based on a Samsung Galaxy S6 (with Android 6.0.1) and the Bluetooth-Scanner App (version 1.1.3) up to 24 m. Also, measurements for moving vehicles were performed. In addition, internal Bluetooth connections of smart phones with the head-unit of the vehicle could be sniffed based on the Ubertooth tool [31], too.

Besides Bluetooth MAC IDs, Wi-Fi MAC ID were analyzed. E.g., the MAC ID of a Wi-Fi hotspot of the head-unit of

TABLE I. CAPTURED AND LOGGED CAM-TRACE, SENSOR DATA TRACE AND VEHICULAR BLUETOOTH ID OF A VEHICLE UNDER SURVEILLANCE WITH AN OBSERVATION DEVICE

CAM Trace	**Sensor Data Trace:** Location, Acceleration, Attitude, Speed, Time	Vehicular Bluetooth **MAC ID**
CAM_1	data $record_1$	48 bit
...	...	...
CAM_n	data $record_n$	48 bit

a BMW 7 at a standstill could be detected based on a Samsung Galaxy S6 (with Android 6.0.1) and the Wifi-Analyzer App (version 3.10.1-L) up to 20 m.

These measurements show that the Secondary Vehicle Identifier, Bluetooth MAC IDs and Wi-Fi MAC IDs of vehicles, are very easy to detect outside of vehicles.

3) Capture Sensor Data Trace of the Observation Device based on the Internal Sensor Elements: Besides communication interfaces smart phones are equipped with additional components (e.g., GPS receiver) and sensor elements (e.g., accelerometer, gyroscope and magnetometer) as already mentioned before. We use these sensors to separately capture geographic location, acceleration, attitude and the according time with the same frequency as CAMs are received. Based on this captured data, the speed can additionally be calculated. If we are doing this, we have two separate data traces, which represent a drive: one CAM-trace and a second trace composed of the captured sensor data termed *sensor-data-trace*, see Table I. Due to the synchronized capturing of both traces (CAM-trace and sensor-data-trace) specific data elements (geographic location, acceleration, attitude, and speed) of both traces can be easily correlated.

VI. Analysis of the Captured Data: CAM-Trace, Sensor-Data-Trace, and Secondary Vehicle Identifier

A. Role of Distinct Pseudonymous ECC Keys

Here, we assume that the pseudonymous ECC keys for V2X are generated at random based on the chosen ECC domain and are securely stored within a secure element in the vehicle and no duplicates of this keys are available. So, a calculation of an ECDSA signature with that key is only possible with the according secure element. Also, the ECDSA signatures will be generated within the secure element to assure a secure application of the ECC key. Moreover, the applied elliptic curve domain parameters (NIST P-256 or BrainpoolP-256r1) are such that ECDSA signatures are not manipulable within the next years. If a CAM (CAM-trace) can be cryptographically verified based on the included certificate (public ECC key) then the CAM (CAM-trace) was signed by the corresponding ECC signing key. In that case, a side effect of cryptographic signing of data is that the transmission of this data is non-disputable.

B. Linking a Captured CAM-Trace to a Vehicle

An attacker knows to which vehicle he sticked the observation device. But further linking mechanism are available based on the captured information, see Section V-B.

1) Linking a Captured CAM-Trace to a Vehicle Based on Secondary Vehicle Identifier: As shown in Section B-B Secondary Vehicle Identifier, e.g., Bluetooth MAC ID of the vehicular head-unit, are very easy to detect. The result is shown in Table I. But in contrast to a signature, a monitored and filed Bluetooth- or Wi-Fi MAC IDs can be altered later on. So, this information is only a reference and no proof of identification.

2) Linking a Captured CAM-Trace to a Vehicle Based on a Physical Fingerprint of the IEEE 802.11p Transmitter: To perform the physical fingerprinting of IEEE 802.11a compliant transmitter, a software defined radio based Wi-Fi sniffer on an Ettus USRP N210 platform was used in [22]. So, the mentioned observation device in Section V-A is not sufficient to extract physical identification features. In [23] an Ettus USRP N210 is used as well to perform physical fingerprinting of IEEE 802.11p compliant transmitter. Physical fingerprinting of transceiver is comparable to an identification of humans based on biometric human features.

3) Linking a Captured CAM-Trace to a Vehicle During an Official Traffic Control: Today, in case of a speeding during an official traffic control, the vehicular speed is measured and photographs are shot of the vehicular driver and the licence plate of the vehicle. In future in addition, CAMs of the crossing vehicles could be recorded and correlated with the optical captured information.

C. Linking a Captured CAM-Trace to a Driver

Among others, people go by vehicle periodically recurring drives. E.g., the daily drive from home to the office, factory or university. These relapsing drives are driver specific and therefore a personal identification feature. So, according CAM-traces can directly be linked to an individual driver.

D. Distinction between a CAM-Trace and a GPS Tracker Observation

Even today an attacker can stick a GPS tracker at a vehicle and monitor and store the geographic position and the according time of a vehicle as a data-trace. But a monitored GPS-trace can be generated by any movement and it is very easy to modify it in some way. So, in contrast to a CAM-trace a GPS data-trace has only minor relevance as proof of a covered drive (to a third party).

E. Distinction between a CAM-Trace and a Personal Observation Performed by a Detective

What is the difference of our observation device to a personal detective who monitors a specific vehicle or person by following the vehicle? The V2V technology provides that ITS vehicle stations will publicly send CAMs to the environment. We have shown, that a standard smart phone with G5 interface will be an adequate observation device. This component is available for everyone. So in future, in contrast to today, more or less “everyone” is able to perform such an observation attack with a smart phone. This means: monitoring and storing CAM-traces, sensor-data-traces, and secondary vehicle identifier (Bluetooth MAC ID, Wi-Fi MAC ID) of any specific ITS vehicle station as presented in Table I.

VII. Conclusion

From our point of view misuse capabilities of the V2V communication arise with the periodically broadcasted CAMs. So, here only CAMs are analyzed.

A. Summary

Privacy problems of the V2V communication - especially CAMs - arise due to the combination of following issues:

- CAMs include static data elements (e.g., length and width of the vehicle, and the confidence level of heading, speed, acceleration, curvature, and yaw rate). Because of this static data, included time stamps and high transmission frequency of up to 10 Hz, subsequent CAMs of a vehicle (Section IV) are linkable to a CAM-trace and
- Cryptographic signing of CAMs (with distinct pseudonymous cryptographic keys) cause non-disputable property of CAMs.

Next, non-disputable CAM-traces can be linked to a specific vehicle (Section VI-B). This is possible based on: Secondary Vehicle Identifier of modern vehicles, e.g.,:

- 64 bit Bluetooth MAC ID of vehicular headunits
- 64 bit MAC ID of vehicle Wi-Fi hotspot (of vehicular headunits)
- Physical fingerprinting of IEEE 802.11p compliant transmitter
- Periodically recurring drives
- ...

and during official traffic controls.

To avoid any privacy problems for drivers with the existing V2V solution, drivers should be selectively able to deactivate V2V transmission of ITS vehicle stations. Moreover, we recommend a standard configuration of V2V transceiver for ITS vehicle stations: radio reception of all CAMs and DENMs but only transmission of DENMs to avoid privacy problems.

B. New V2V Approach for Day-2

Research and development of the V2V communication has started 15 years ago. In the meantime, the IT architecture of vehicles has significantly changed. A lot of components for assisted driving are available: lane keeping support, traffic jam assist, automatic parking assistants, remote parking assistants and so on. This is a pre-stage of automatic driving, which is one of the main challenges in automotive engineering at the moment. Already, the mentioned systems to support driving require specific sensor systems to detect objects (e.g., road lanes, other vehicles and/or static traffic signs) as well as pedestrians and bicycles by capturing the environment. Many modern vehicles are already able to deduce a specific environmental traffic situation based on the captured information without any V2V communication. The integration of further sensor elements in vehicles is an ongoing activity due to automated driving in the near future. We argue that due to this deployment the relevance of the V2V communication will change over time.

To avoid the misuse of CAMs to harm privacy a selective communication approach for CAMs should be chosen instead of todays continuous communication of CAMs. E.g., CAM transmission on location with statistical higher accident rates, on crossings, during passing maneuver, etc. In addition, the amount of included data in CAMs should be restricted. Furthermore, a new cryptographic concept should be chosen which avoid the non-disputable property of CAMs today.

From a technical perspective, the current V2V concept, signing CAMs on the sender side and verifing CAMs on the receiver side, is very time consuming. In addition, a complex key management system is necessary to enrole the needed pseudonymous certificates. Moreover, the integration of ECDSA-signature and certificate expands the CAM message size tenfold - see Section III-A1 - and can cause CAM collisions on the wireless communication cannel. This effect will dramatically increase, when a switch to another ECC domain parameter set (e.g., NIST P-386 [10] or BrainpoolP386r1 [11]) is needed for security reasons in future.

C. V2X Communication

In this paper, only the V2V communication, especially CAMs, are analyzed. In contrast, the adaptation of the ETSI communication to ITS roadside station - constituted in [32] - is sound and can be broadly applied that way.

VIII. Acknowledgement

The authors would like to thank our colleague Gerd Nolden for the discussion and our student Tobias Franz for performing real measurements of Secondary Vehicle Identifier. Also thanks to the anonymous reviewers for the valuable comments.

References

[1] Markus Ullmann, Thomas Strubbe, and Christian Wieschebrink, "Technical Limitations, and Privacy Shortcomings of the Vehicle-to-Vehicle Communication," in Proceedings VEHICULAR 2016: The Fifth International Conference on Advances in Vehicular Systems, Technologies and Applications. IARIA, 2016, pp. 15–20.

[2] ——, "V2V Communication - Keeping You Under Non-Disputable Surveillance (Short Paper)," in Proceedings of the IEEE Vehicular Networking Conference (VNC). IEEE, 2016.

[3] Car 2 Car Communication Consortium, "Mission, News, Documents," 2015, https://www.car-2-car.org/, access date: November 02, 2016.

[4] ETSI, "Intelligent Transport Systems (ITS); Security Header and Certificate Formats; ETSI TS 103 097 V1.2.1," 2013, http://www.etsi.org/, access date: November 02, 2016.

[5] European Commission, "SCOOP@F," 2013, http://inea.ec.europa.eu/en/ten-t, Access Date: June 2, 2017.

[6] BMVI, "Cooperative ITS Corridor Rotterdam-Franfurt-Vienna Joint deployment," 2014, http://www.bmvi.de, Access Date: June 2, 2017.

[7] Vejdirektoratet, "NordicWay," 2016, http://vejdirektoratet.dk/EN/roadsector/Nordicway/Pages/Default.aspx, access date: November 2, 2016.

[8] European Commission, "Strategy Towards Cooperative, Connected and Automated Mobility," 2016, http://ec.europa.eu/transport/themes/its/news/2016-11-30-c-its-strategy_en, access date: November 30, 2016.

[9] C-ITS Platform of the EC DG MOVE, "Final Report," 2016, http://ec.europa.eu/transport/themes/its/doc/c-its-platform-final-report-january-2016.pdf, access date: November 2, 2016.

[10] Recommended Elliptic Curves For Federal Government Use, National Institute of Standards and Technology, 1999. [Online]. Available: http://csrc.nist.gov/groups/ST/toolkit/documents/dss/NISTReCur.pdf, access date: November 02, 2016

[11] Brainpool, "ECC Brainpool Standard Curves and Curve Generation, Version 1.0," 2005, http://www.ecc-brainpool.org/ecc-standard.htm, access date: November 02, 2016.

[12] G. Samara, W. A. Al-Salihy, and R. Sures, "Security Analysis of Vehicular Ad Hoc Nerworks (VANET)," in Network Applications Protocols and Services (NETAPPS), 2010 Second International Conference on. IEEE, 2010, pp. 55–60.

[13] P. Papadimitratos, L. Buttyan, J.-P. Hubaux, F. Kargl, A. Kung, and M. Raya, "Architecture for Secure and Private Vehicular Communications," in Telecommunications, 2007. ITST'07. 7th International Conference on ITS. IEEE, 2007, pp. 1–6.

[14] J. Freudiger, M. Raya, M. Félegyházi, P. Papadimitratos et al., "Mix-Zones for Location Privacy in Vehicular Networks," in Proceedings of the first international workshop on wireless networking for intelligent transportation systems (Win-ITS), 2007.

[15] J. Petit, F. Schaub, M. Feiri, and F. Kargl, "Pseudonym schemes in vehicular networks: A survey," IEEE communications surveys & tutorials, vol. 17, no. 1, 2015, pp. 228–255.

[16] B. Wiedersheim, Z. Ma, F. Kargl, and P. Papadimitratos, "Privacy in Inter-Vehicular Networks: Why Simple Pseudonym Change is not Enough," in Wireless On-demand Network Systems and Services (WONS), 2010 Seventh International Conference on Wireless On-demand Network Systems and Services. IEEE, 2010, pp. 176–183.

[17] S. S. Yang, Y. G. Kim, and H. Choi, "Vehicle Identification using Discrete Spectrums in Wireless Sensor Networks," Journal of Networks, vol. 3, no. 4, 2008, pp. 51–63.

[18] S. Astapov and A. Riid, "A Multistage Procedure of Mobile Vehicle Acoustic Identification for Single-Sensor Embedded Device," International Journal of Electronics and Telecommunications, vol. 59, no. 2, 2013, pp. 151–160.

[19] C. Carpenter, M. Fowler, and T. Adler, "Generating Route-Specific Origin-Destination Tables Using Bluetooth Technology," Transportation Research Record: Journal of the Transportation Research Board, no. 2308, 2012, pp. 96–102.

[20] Markus Ullmann, Tobias Franz, and Gerd Nolden, "Vehicle Identification Based on Secondary Vehicle Identifier - Analysis, and Measurements -," in Proceedings VEHICULAR 2017: The Sixth International Conference on Advances in Vehicular Systems, Technologies and Applications. IARIA, July 2017.

[21] B. Danev, D. Zanetti, and S. Capkun, "On Physical-Layer Identification of Wireless Devices," ACM Computing Surveys (CSUR), vol. 45, no. 1, 2012, p. 6.

[22] T. D. Vo-Huu, T. D. Vo-Huu, and G. Noubir, "Fingerprinting Wi-Fi Devices Using Software Defined Radios," in Proceedings of the 9th ACM Conference on Security and Privacy in Wireless and Mobile Networks. ACM, 2016, pp. 3–14.

[23] G. Baldini, R. Giuliani, and E. Cano Pons, "An analysis of the privacy threat in vehicular ad hoc networks due to radio frequency fingerprinting," Mobile Information Systems, vol. 2017, 2017.

[24] C. Han, M. Dianati, R. Tafazolli, R. Kernchen, and X. Shen, "Analytical Study of the IEEE 802.11p MAC Sublayer in Vehicular Networks," IEEE Transactions on Intelligent Transportation Systems, vol. 13, no. 2, 2012, pp. 873–886.

[25] Q. Wang, S. Leng, H. Fu, and Y. Zhang, "An IEEE 802.11p - based Multichannel MAC Scheme with Channel Coordination for Vehicular Ad Hoc Networks," IEEE Transactions on Intelligent Transportation Systems, vol. 13, no. 2, 2012, pp. 449–458.

[26] S. Eichler, "Performance Evaluation of the IEEE 802.11p WAVE Communication Standard," in Vehicular Technology Conference, 2007. VTC-2007 Fall. 2007 IEEE 66th. IEEE, 2007, pp. 2199–2203.

[27] ETSI, "ETSI EN 302 665 V1.1.1: Intelligent Transport Systems (ITS) - Communications Architecture," 2010, http://www.etsi.org/, Access Date: June 02, 2017.

[28] ——, "ETSI EN 302 637-2 V1.3.2: Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service," 2015, http://www.etsi.org/, Access Date: June 02, 2017.

[29] ——, "ETSI TS 102 637-3 V1.2.2: Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service," 2010, http://www.etsi.org/, access date: November 02, 2016.

[30] T. Franz, "Bachelor Thesis: Drahtlose Identifier in modernen Fahrzeugen," Univerity of Applied Sciences Bonn-Rhine-Sieg, 2016.

[31] M. Herrmann, "Ubertooth-Bluetooth Monitoring und Injection," Network, vol. 19, 2013.

[32] Markus Ullmann, and Thomas Strubbe, and Christian Wieschebrink, and Dennis Kügler, "Secure Vehicle-to-Infrastructure Communication: Secure Roadside Stations, Key Management, and Crypto Agility," in International Journal On Advances in Security, vol 9 no 12. IARIA, 2016, pp. 80–89.

TABLE II. DIFFERENCES OF V2V IN EUROPE AND US

	Europe	**US**
Standards:	ETSI 102637 1-3	SAE J 2735
	ETSI 102 943	IEEE 1609.2
	ETSI 103 097 (Naming derived from IEE 1609.2)	
	further ETSI standards possible	
Accepted ECC Curves:	NIST P-256r1	NIST P-256r1
	BrainpoolP256r1 (in discussion)	BrainpoolP256r1 (in discussion)
Message Types:	CAM	BSM
	DENM	RSA
		EVA
	"unlimited" number of types possible	limited number of types
Minimal Message Size without Signature and Certificate:	186 bit	275 bit
Minimal Message Size with Signature and Certificate:	˜2 Kbit	˜2 Kbit

[33] SAE, "SAE J2735: Dedicated Short Range Communications (DSRC) Message Set Dictionary (issued 2015-09, revised 2016-03)," 2016, http://www.SAE.org/.

[34] IEEE, "IEEE 1609.2: Standard for Wireless Access in Vehicular Environments Security Services for Applications and Management Messages," 2016, http://www.IEEE.org/.

[35] R. M. Ishtiaq Roufa, H. Mustafaa, S. O. Travis Taylora, W. Xua, M. Gruteserb, W. Trappeb, and I. Seskarb, "Security and privacy vulnerabilities of in-car wireless networks: A tire pressure monitoring system case study," in 19th USENIX Security Symposium, Washington DC, 2010, pp. 11–13.

APPENDIX A
DIFFERENCES OF THE V2V COMMUNICATION IN EUROPE AND US

The V2V communication according to ETSI and the US standards, SAE J2375 (revised 2016-03)[33] and IEEE 1609.2 [34], use similar concepts, both are based on IEEE 802.11p, but there are small and major differences between both approaches. While the European standardization work in this area is exclusively executed by ETSI, the US standards are executed by IEEE as well as SAE.

One difference concerns the message types broadcasted by the ITS stations. In either case, vehicles send pseudonymously signed messages. But in the US instead of CAMs, Basic Safety Messages (BSMs) are sent. Both contain mostly identical data fields, but differ in precision. E.g., in CAMS the vehicle sizes are stated in rather vague decimeters, whereas in BSMs vehicle sizes are stated in more precise centimeters.

There is no direct equivalent to the DENM in the US standards. Comparable are the Roadside Alerts (RSA), which are used to inform receivers about certain events in the area, e.g., an approaching train or icy roads. Based on those, emergency vehicles send emergency vehicle alert (EVA), that also contain the type of the vehicle. In contrast to DENMs in Europe, RSAs and EVAs will not be transmitted by an hop-by-hop mechanism. So, those location based warnings can only be received in proximity to the location. BSMs and other messages used in the US have a larger payload than their european counterparts, but due to certificates and signatures their overall size is not significantly larger.

The used cryptographic concepts are quite similar. In Europe as well an in US the signature algorithms ECDSA will be used. In the US standards the ECC domain NIST P-256 and

BrainpoolP-256r1 are defined for usage whereas the ETSI standards only provide NIST P-256. There are discussions beside the formal standards concerning ECC domain parameters: In the US to drop BrainpoolP-256r1 ECC domain parameters and in Europe to accept BrainpoolP-256r1 ECC domain parameter. Similar as well is the message frequency. CAMs and BSMs are both sent with a frequency of up to 10 Hz. A pseudonym change frequency is neither in the US nor European standards specified.

APPENDIX B
ITS VEHICLE IDENTIFIER

The term ITS vehicle identifier is completely independent from the V2V communication.

Here, we categorize the available identifiers of vehicles into three different classes. Primary vehicle identifier represent such identifiers which will be typically regarded today, e.g., the Vehicle Identification Number (VIN). Secondary Vehicle Identifier come up with new information technologies used in modern vehicles. Tertiary vehicle identifier are not sufficient to directly identify a vehicle but to link CAM respective DENM messages of an ITS vehicle station.

A. Primary Vehicle Identifier

To date, each vehicle is identifiable based on the distinct VIN. In some areas the VIN is integrated as human readable information in the windscreen of vehicles.

Besides the VIN, vehicles are marked with a licence plate. This is a further primary vehicle identifier, which is already used for identification.

With the deployment of the V2V technology vehicles will be equipped with a long term ECC key pair and an appropriate certificate. This certificate becomes an additional primary vehicle identifier.

B. Secondary Vehicle Identifier

Besides these obvious primary vehicle identifiers, vehicles have further identifiers. Modern vehicles are equipped with multi-media components, which are able to etablish communications with electronic devices of the driver or passengers. Typically, wireless communication technologies, e.g., Bluetooth, are used for that purpose.

A Bluetooth multi-media device emits a static 48 bit MAC identifier. The MAC ID is composed of two parts: the first half is assigned to the manufacturer of the device, and the second half is assigned to the specific device. In addition, each Bluetooth device emits a "User-friendly-name" which is typically alterable. Bluetooth devices operate in the ISM band (2.4 to 2.485 GHz).

Secondary Vehicle Identifier have no formal character in contrast to a licence plate or VIN. But it is technically very easy to capture Bluetooth MAC IDs and SSIDs of a vehicle and to link them to a vehicle because their primary application is to establish a communication with other devices. So, attacker can use them for their purpose.

Moreover, vehicle head-units allow any Wi-Fi equipped laptop, tablet or mobile phone to access the internet within the ITS vehicle station while travelling if the head-unit has mobile communications capabilities. But head-units configured as access point need an unique Service Set Identifier (SSID) or network name to connect devices. According to the IEEE 802.11 workgroup, Wi-Fi can be used in following distinct frequency ranges: 2.4 GHz, 3.6 GHz, 4.9 GHz, 5 GHz, and 5.9 GHz bands. Each range is divided into a multitude of channels. Countries apply their own regulations to the legitimate channels and maximum power levels within these frequency ranges. In addition, each head-unit needs an unique MAC address. This is a further Secondary Vehicle Identifier.

If vehicles are equipped with mobile communication capabilities an International Mobile Subscriber Identity (IMSI) is required. That is an unique identification number to identify a mobile device within the network. In addition, a SIM card with an assigned mobile phone number is needed for mobile communication.

MAC IDs of Bluetooth interfaces respective Wi-Fi access points are detectable very easy with every smart phone [20].

Since the 1th of November 2014, vehicles and motorhomes have to be equipped with a Tire Pressure Monitoring System (TPMS) within Europe. TPMS can be dived in direct and indirect TPMS. Direct TPMS means that specific physical sensors measure the air pressure of the tires. These sensors communicate wireless with the vehicle and transmit an identifier of 28 to 32 bit length. There are different wireless technologies available for 125 kHz or 315 kHz respective 433 MHz. A detection range of up to 40 m for direct TPMS is mentioned in [35].

In [22] the physical fingerprinting of IEEE 802.11a compliant transmitter is investigated. As physical identification features the transmitter individual scrambling seed, carrier frequency offset, and sampling frequency offset are used. For some IEEE 802.11a transmitter an identification accuracy, based on these physical identification features, of up to 100 % is reported. IEEE 802.11p is technically very similar to IEEE 802.11a. A physical fingerprinting of IEEE 802.11p compliant transmitters is analyzed in [23].

So far mentioned vehicle identifiers are sufficient for identification all the time. Furthermore, there exists vehicle identifier with a limited validity period, e.g., pseudonymous certificates (termed authorization tickets by ETSI).

C. Tertiary Vehicle Identifier

CAMs contain a lot of static information, like the vehicle length and vehicle width and the confidence level of heading, speed, acceleration, curvature, and yaw rate. These information enable to link CAMs only based on the CAM data elements.