Technical Limitations, and Privacy Shortcomings of the Vehicle-to-Vehicle Communication

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-to-Vehicle communication technology according to ETSI is in preparation in Europe. Currently, a Public Key Infrastructure policy for Intelligent Transport Systems in Europe is in discussion to enable V2V communication. This policy set aside two classes of keys and certificates for ITS vehicle stations: long term authentication keys and pseudonymous keys and certificates. We show that from our point of view the periodic sent Cooperative Awareness Messages with extensive data have technical limitations and together with the pseudonym concept cause privacy problems.**

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

I. Introduction

Vehicle-to-vehicle (V2V) and vehicle-to-infrastructure communication (V2I) (consolidated V2X) have been discussed intensively 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[1]. This includes the security standardization as well [2].

The ETSI specifications define an architecture for Intelligent Transport Systems (ITS). This architecture defines 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 defined for information exchange. Primary, these are the Cooperative Awareness Message (CAM) and the Decentralized Environmental Notification Message (DENM). These messages are disseminated via broadcast. According the ETSI specifications messages 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 [3] in France, the C-ITS corridor Rotterdam-Frankfurt-Vienna [4] and the Nordic Way [5], a joint project of Denmark, Finland, Norway, and Sweden.

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 to assist driving are available: lane keeping support, traffic jam assist, automatic parking assistant, remote parking assistant and so on. This is a prestage 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 of the sensor elements without any V2V communication. But 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. So on the one side, the importance of the periodically sent CAM, to deduce a specific environmental traffic situation, will decrease to more or less additional information in consequence of the integration of sensor systems in vehicles. On the other side, the signing of the CAM data and the integration of the certificate expands the message size tenfold, which can cause message collisions on the wireless communication cannel.

In the final report of the C-ITS platform (January 2016) of the EC DG MOVE the data elements of CAM and DENM messages of ITS vehicle stations are rated as *personal data* [6]. To put it briefly, 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 this paper, we show that it is easy to link CAMs of a vehicle to a CAM trace even in case of a pseudonym switch. The effect of cryptographic signed CAMs is that the existance of the CAM data is not disputable. The applied cryptographic ECC domain parameter (NIST P-256 [7], BrainpoolP-256r1 [8]) are such that ECDSA signatures are not foregable within the next years. Assuming, an attacker can plot a CAM trace of a vehicle. Is there any evidence that only one CAM of the whole CAM trace can be bound to a specific vehicle then the whole CAM trace can be bound to this vehicle. The attack to capture CAM traces and to bind these to a specific vehicle respective driver is described in [9]. So, CAMs provide side effects which can totally jeopardize the privacy of motorist. The technical limitations and the privacy shortcomings are raised by the usage of electronic signatures to assure message integrity and authentication.

Besides sensor elements, modern vehicles are equipped with wireless interfaces, e.g., bluetooth to connect devices (smart phones, tablets, etc) to the multimedia component of the vehicle. Initially, these wireless interfaces have nothing to do with the V2V communication. But from an attacker perspective these interfaces enable to bind captured CAM data traces to a specific vehicle. Therefore, these wireless vehicular interfaces has to be regarded in a holostic 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. Subsequent, identifiers for ITS vehicle stations are presented in Section IV. Next, technical limitations and privacy shortcomings of the current V2V communication approach are illustrated in Section V. Finally, in Section VI we summarize our results.

II. Related Work

A detailed overview of attacks in VANETs is given by Ghassan Samara et al. in [10]. A security and privacy architecture for pseudonymous message signing is described in [11]. Here, a public key infrastructure is regarded, too. In [12], Julien Freudiger et al. suggested mix zones for location privacy in vehicular networks. Giorgio Calandriello et al. propose onboard, on-the-fly pseudonym certificate generation and self-certification. The autors developed this approach to alleviate one of the most significant limitations of the pseudonym-based approach: the need for complex management. To achieve this, the use of group signatures is proposed. A survey on pseudonym schemes in vehicular networks is given in [13].

A detailed analysis of privacy requirements and a comparison with the security requirements in VANETs is given in [14]. Wiedersheim et al. [15] analyzed the location privacy in a specific communication scenario. Vehicles send beacon messages periodically. 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 the attacker is able to track the vehicles with an accuracy of almost 100% if he uses the approach in [15]. 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)

The fleet of ITS vehicle stations is equipped with additional V2V communication gateways only for monitoring the ambient V2V communication. All the collected data is sent to a centralized server infrastructure to analyze the data. Primary use case can be the analysis of traffic flow for the fleet to perform optimized navigation for individual ITS vehicle stations.

Besides the identification of ITS vehicle station 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 [16] [17]. They differ in concerning single or multi sensor usage and concrete feature extraction. Surprisingly, neither common security nor privacy analyzation 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 vehicles counting on specific roads. In [18], an analysis in Jacksonville, Florida, is described. Therefore, a set of Bluetooth receivers was located at the roadside on specific streets to capture the Bluetooth MAC ID of crossing vehicles. But no paper is found, which analyze the ultimate problem of the usage of signatures to assure CAM integrity and authenticity. That issue is addressed here.

III. Secure V2X Communication

The ETSI specification [19] defines a basic set of applications for ITS, like active road safety (e.g., emergency vehicle warning), co-operative traffic effiency (e.g., regular speed), co-operative local services (e.g., automatic access control), and global internet services (e.g., fleet management).

To date, V2X broadcast communication based on IEEE 802.11p is provided. So, V2X is a short range communication technology with a communication range of about 600 m in open space.

The ETSI ITS architecture [19] 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: Cooperative Awareness Message, and Dezentralized Environmental Notification Message.

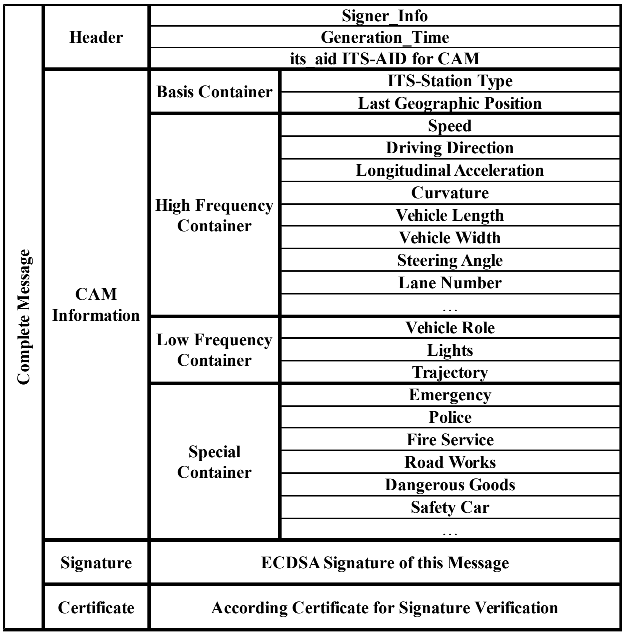
ITS stations will be equipped with two classes of key pairs/certificates:

1) Long term key pairs (certificates) based on elliptic curve cryptography (ECC)
2) Pseudonymous ECC key pairs (certificates)

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). Pseudonymous keys are used to secure the CAMs and DENMs mentioned in Section III-A respective Section III-B. It is assumed that pseudonymous keys and certificates are not directly linkable to an identity of an ITS vehicle station.

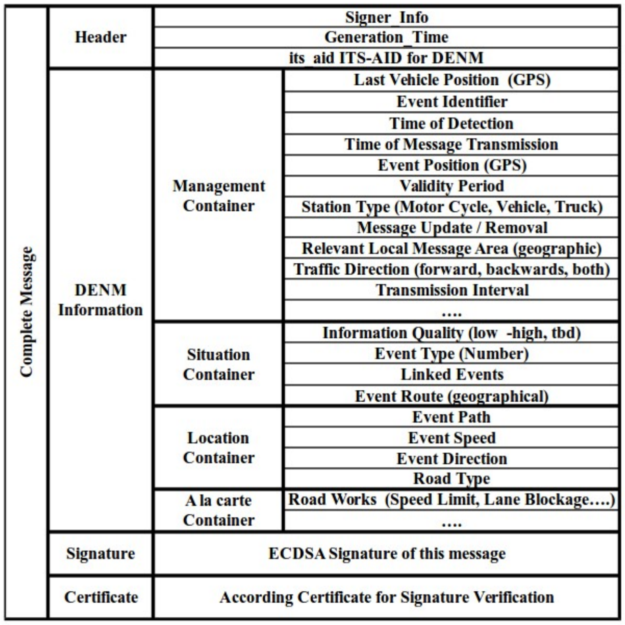
A. Cooperative Awareness Message

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



Complete Message	Header		Signer_Info
			Generation_Time
			its_aid ITS-AID for CAM
	CAM Information	Basis Container	ITS-Station Type
			Last Geographic Position
		High Frequency Container	Speed
			Driving Direction
			Longitudinal Acceleration
			Curvature
			Vehicle Length
			Vehicle Width
			Steering Angle
			Lane Number
			…
		Low Frequency Container	Vehicle Role
			Lights
			Trajectory
		Special Container	Emergency
			Police
			Fire Service
			Road Works
			Dangerous Goods
			Safety Car
			…
	Signature	ECDSA Signature of this Message	
	Certificate	According Certificate for Signature Verification	

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



Complete Message	Header		Signer_Info
			Generation_Time
			its_aid ITS-AID for DENM
	DENM Information	Management Container	Last Vehicle Position (GPS)
			Event Identifier
			Time of Detection
			Time of Message Transmission
			Event Position (GPS)
			Validity Period
			Station Type (Motor Cycle, Vehicle, Truck)
			Message Update / Removal
			Relevant Local Message Area (geographic)
			Traffic Direction (forward, backwards, both)
			Transmission Interval
			….
		Situation Container	Information Quality (low -high, tbd)
			Event Type (Number)
			Linked Events
			Event Route (geographical)
		Location Container	Event Path
			Event Speed
			Event Direction
			Road Type
		A la carte Container	Road Works (Speed Limit, Lane Blockage….)
			….
	Signature	ECDSA Signature of this message	
	Certificate	According Certificate for Signature Verification	

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.

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 confidence levels of heading, speed, acceleration, curvature and yaw rate and the length and width of the ITS vehicle station are given. Length and width are stated with a precision of 10 centimeters.

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 chosen. Then the receiver is able to cryptographically verify the message and check the temporal validity (temporary freshness).

It is not planned to forward CAM messages hop-to-hop. Figure 1 illustrates the structure of a Cooperative Awareness Message. The CAM is specified in detail in [20].

Regarding ECDSA based on the ECC domain parameter 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 [2]. So, only about 10 % of the whole CAM message size are needed 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.

B. *Dezentralized Environmental Notification Message*

In contrast, the second message type, Dezentralized Environmental Notification Messages (DENMs), are event-driven and indicate a specific safety situation, e.g., road works warning (from an ITS roadside station) or a damaged vehicle warning (from an ITS vehicle station). The DENM message format is specified in detail in [21]. DENM messages can be transmitted hop-by-hop. Figure 2 illustrates the structure of a Dezentralized Environmental Notification Message.

C. *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. The used key for signing and the appropriate certificate are periodically changed during operation. Therefore, an ITS vehicle station needs a set of pseudonymous keys and certificates valid for some period of time. The set size of pseudonymous keys and certificates and the pseudonym change frequency are not specified in [22].

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

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.

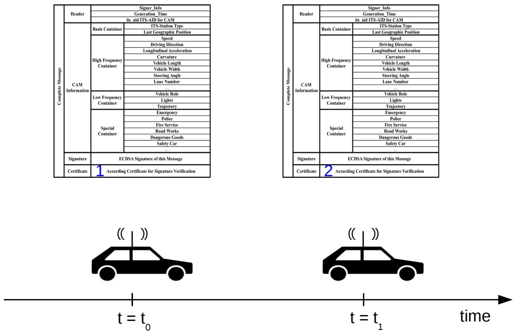


Figure 3. Switch pseudonymous keys for signing CAMs respective DENMs (pseudonym concept)

IV. ITS Vehicle Identifier

Here, we categorize the available identifiers of vehicles into three 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).

Moreover, vehicle-based wireless routers allow any Wi-Fi equipped laptop, tablet or mobile phone to access the internet within the ITS vehicle station while travelling if the router has mobile communications. But routers 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 wireless router has an unique MAC address. This is a further secondary vehicle identifier.

A Wi-Fi access point is accompanied by mobile communication. Mobile communication requires an International Mobile Subscriber Identity (IMSI). 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.

Since the 1^{th} of November 2014, vehicles and motorhomes have to be equipped with a Tyre Pressure Monitoring System (TPMS) within Europe. There exists direct and indirect TPMS. Direct TPMS means that specific physical sensors measure the air pressure of the tyres. 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 [23].

Initially, 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.

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 static information enable to link CAMs only based on the CAM data elements.

V. Analyzation of the V2V communication

From our point of view the main technical- and privacy problems arise with the periodically broadcasted CAMs. So, here in our analysis only CAMs are addressed.

A. *Technical Issues*

1) CAM data elements: A lot of CAM data elements are results of sensor measures, like: speed, driving direction, longitudinal acceleration, curvature. But sensors have only a defined precison level.

The geographic position is typically calculated based on satellite systems, like GPS. But spoofing attacks on GPS to influence the geographic position are possible. This issue is intensively analyzed in Tippenhauer et al. [24]. Open source code for software definded radio makes GPS spoofing attacks very realistic. The tool GPS-SDR-SIM generates GPS baseband signal data streams, which can be converted to RF using software-defined radio (SDR) platforms, such as bladeRF, HackRF, and USRP [25]. In addition, spoofing attacks on GPS can also influence the time synchronization for ITS vehicle stations.

For that, the data elements of received CAMs can only be regarded as additional information, which have to be verified by internal sensor measurements of the ITS vehicle station. Even when a receiver can cryptographically verify a

CAM respective DENM then the receiver only knows that the received data is broadcasted by an authentic ITS station and no error happend on the wireless transmission path of the data. Nevertheless the receiver can not really trust the CAM data due to the sensor accuracy and possibly attacks on the time value and geographic position as well as modifications of vehicular components.

2) Capacity of the IEEE802.11p channel: As shown in III-A only about 10% of the CAM size is used for coding the data, the remainder to assure integrity and authenticity of the data (ECDSA signature and certificate). So, the used technology to assure message authentication and integrity is very costly especially considering the fuzziness of the CAM data as shown in V-A1.

Even today collisions on the IEEE802.11p channel are feared in case of a large number of communicating ITS vehicle stations in a local area because all ITS station share only one frequency channel for the whole broadcast communication. But obviously we have to adapt the used key length to perform the ECDSA signature in future. Today, the NSA does not recommend to use the ECC domain NIST P-256 any more, due to the progress in quantum computing [26]. The next existing ECC domain parameters have key length of 384 bit. This extends the size of ECDSA signature from 512 to 768 bit. This means the CAM size will be increased from 2 kbit to 2,5 kbit because the signature of the certificate is affected, too. This will worsen the collision problem. Looking in the remote future (20 year ahead) we have to regard that quantum computers can possibly attack elliptic curve cryptography. There is large progress in research and construction of quantum computers based on semiconductors at the moment. Because vehicles have an operation time of about 15 - 20 years that issue has to be regarded in future, too. Although, no broadly accepted alternative post-quantum public key cryptography is ready for application, one consequence is very certain: in future new post-quantum public key cryptography have to use much longer keys compared to ECC today. This worsen the collision problem if ECDSA signatures should be replaced by post-quantum signatures algorithms.

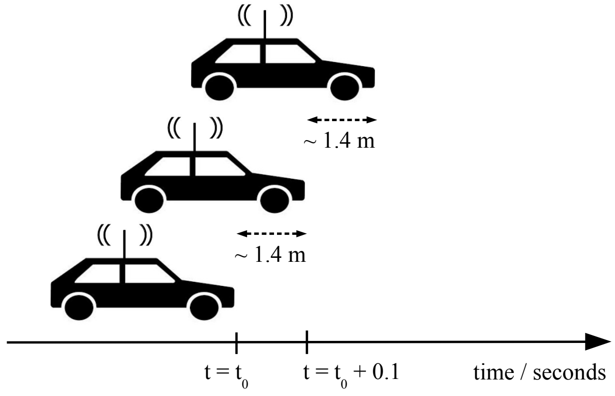
B. Security Issues

1) Jamming the IEEE802.11p channel: An attack, which can be performed very easy is jamming the 5.9 GHz wireless channel (with a strong sender). As consequence, it can not be assured that CAM and DENM messages reach the surrounded ITS vehicle stations in time.

2) Security Shortcomings of the ETSI Specifications: The ETSI certificate format provides only elliptic curve cryptography based on the NIST prime curve P-256. No mechanism is provided to securely adapt the key length or ECC domain parameters or cryptographic algorithms if necessary. In the meantime this issue is already termed: cryptographic agility. Additional security shortcomings concerning the necessary Public Key Infrastructure are explained in detail in [27].

C. Privacy Issues

1) Linkability of CAMs based on Certificates: Each CAM includes a pseudonymous certificate. The appropriate 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 appropriate certificate is static. So, this static information at the end of each CAM can be easily used to link 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.



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

D. Linkability of CAMs based on the CAM data

The requested transmission rate for CAMs are 10 messages per 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 an ITS vehicle station has a minimum length of 3 m: In that case the length of an ITS vehicle station overlaps at least 50% of the movement (1.4 m). 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. This means, a linkability of CAMs of a specific ITS vehicle station is constituted only based on the geographic position of the CAMs respective DENMs. In addition, further static CAM data elements (e.g., vehicle length and vehicle width, and the confidence level of heading, speed, acceleration, curvature, and yaw rate) and the current speed (minor change within a time frame of 100 ms) are helpful to link the CAMs if the ITS vehicle station is much faster then 50 km/h. Furthermore, the trajectory (included in the low frequency container of the CAM) can be used to link CAMs of an ITS vehicle station.

These linkability of CAMs can be exploited to plot complete CAM traces of drives of a specific vehicle described in detail in [9].

Also, CAM traces can be bound to a vehicle, e.g, based on secondary identities. First practical measurements show that, e.g., bluetooth multi-media devices of analyzed vehicles of a specific german OEM have the “User-friendly-name” *OEM name* followed by a *figure space* and an individual five-figure number. The *five-figure number* are the last 5 figures of the VIN.

VI. Conclusion

Modern vehicles are already equipped with a lot of sensor elements to support driving assistance. That will be an ongoing process due to automated driving. ITS vehicle stations can trust data of internal vehicular sensors much more than the information contained in the received CAMs as shown in V-A. Additionally, an ITS vehicle station can not be sure that sent CAMs can be received in time, due to jamming or collisions on the wireless communication channel. For the reasons listed above, we argue that the V2V communication, especially CAMs, will not have this importance then expected. CAM data can only be an additional information, e.g., in invisible situations which have to be checked by the internal sensors. In addition, the concept to secure messages (ECDSA signature) and to verify them is very time consuming. In addition, a complex key management system is necessary to enrole the needed pseudonymous keys and certificates. Moreover, the signing of the data increase the CAM message size by a factor of 10. Finally, the mechanism to solve the privacy requirements (pseudonym concept) allows attackers to plot CAM traces of specific vehicles and drivers, which are non-disputable, due to the applied signatures with unique keys. So, the suggested pseudonym concept neglects the privacy requirements. In summary, it can be stated that a new V2V approach for the day-2 deployment of ITS vehicle stations is needed, which addresses the whole analyzed technical limitations and privacy shortcomings of the periodic sent CAMs. One possible direction is to use symmetric cryptography (message authentication codes) instead of electronic signatures, mentioned in [13].

In this paper, only the V2V communication, especially CAMs, are analyzed. In contrast, the adaptation of the ETSI communication to ITS roadside station - vehicle-2-infrastructure (V2I) - constituted in [27] is sound and can be broadly applied that way.

References

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

[2] ETSI, “Intelligent Transport Systems (ITS);Security; Security header and certificate formats, ETSI TS 103 097 V1.2.1,” 2013, http://www.etsi.org/, access date: November 02, 2016.

[3] European Commission, “SCOOP@F,” 2013, http://inea.ec.europa.eu/en/ten-t, access date: November 2, 2016.

[4] BMVI, “Cooperative its corridor rotterdam-franfurt-vienna joint deployment,” 2014, http://www.bmvi.de, access date: November 2, 2016.

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

[6] 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.

[7] 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

[8] Brainpool.

[9] M. Ullmann, T. Strubbe, and C. Wieschebrink, “V2V Communication - Keeping You Under Non-Disputable Surveillance (Short Paper),” in Proceedings of the IEEE Vehicular Networking Conference(VNC), to appear. IEEE, 2016.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] F. Schaub, Z. Ma, and F. Kargl, “Privacy requirements in vehicular communication systems,” in Computational Science and Engineering, 2009. CSE’09. International Conference on, vol. 3. IEEE, 2009, pp. 139–145.

[15] 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. IEEE, 2010, pp. 176–183.

[16] 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.

[17] 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.

[18] 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.

[19] ETSI, “ETSI EN 302 665 V1.1.1: Intelligent Transport Systems (ITS) - Communications Architecture,” 2010, http://www.etsi.org/, access date: November 02, 2016.

[20] ——, “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: November 02, 2016.

[21] ——, “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.

[22] N. Bissmeyer, H. Stubing, E. Schoch, S. Gotz, J. P. Stotz, and B. Lonc, “A generic public key infrastructure for securing car-to-x communication,” in 18th ITS World Congress, 2011.

[23] 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.

[24] N. O. Tippenhauer, C. Pöpper, K. B. Rasmussen, and S. Capkun, “On the requirements for successful gps spoofing attacks,” in Proceedings of the 18th ACM conference on Computer and communications security. ACM, 2011, pp. 75–86.

[25] T. Ebinuma, “Gps-sdr-sim,” GitHub, 2015, https://github.com/osqzss/gps-sdr-sim, access date: Novemver 2, 2016.

[26] National Security Agency, “Cryptography today,” 2015, https://www.nsa.gov/ia/programs/suiteb_cryptography, access data: November 02, 2016.

[27] M. Ullmann, T. Strubbe, C. Wieschebrink, and D. 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.