On Handling of Certificate Digest in V2X Communication

Takahito Yoshizawa
imec-COSIC KU Leuven
Kasteelpark Arenberg 10 Bus 2452
Leuven, B-3001, Belgium
takahito.yoshizawa@esat.kuleuven.be

Bart Preneel
imec-COSIC KU Leuven
Kasteelpark Arenberg 10 Bus 2452
Leuven, B-3001, Belgium
bart.preneel@esat.kuleuven.be

***Abstract*—We propose a change in the IEEE 1609.2 and ETSI ITS standards that define a certificate distribution mechanism, called *inline peer-to-peer certificate distribution (P2PCD)*. Messages exchanged in V2X messages are secured with digital signatures and digital certificates for the corresponding public keys. This *P2PCD* mechanism is used in Basic Safety Message (BSM) for the US and Cooperative Awareness Message (CAM) for Europe, and allows vehicles to proactively resolve unknown certificates. The unknown certificate situation occurs as not all messages contain the certificate in order to reduce overhead in these messages. This mechanism appears to be beneficial to minimize delay in verifying the authenticity and integrity of received messages. We evaluated its usefulness by conducting a simulation to recreate real-world highway traffic flow. The result indicates that, for high-way traffic, the benefit of this mechanism is negligble. At the same time, it increases unnecessary processing burden in vehicles. Based on our observation, we propose to update the IEEE 1609.2 and ETSI ITS standards in such a way that this mechanism should be restricted to traffic environments where it brings benefits.**

***Index Terms*—Vehicular communication, V2X, PKI, Certificate, BSM, CAM**

I. Introduction

Vehicular communications and autonomous driving vehicles have been gaining increasing attention in recent years [19]. At the same time, both industry and academia raise concerns on cybersecurity aspects of so-called *connected vehicles*, or Vehicle-to-Everything (V2X) and challenges that lie ahead [7], [16]. To ensure coordinated implementations and deployments, standard bodies such as IEEE and ETSI have published specifications on vehicular communications. These standards include: (1) the IEEE 1609 series called Wireless Access in Vehicular Environments (WAVE), (2) IEEE 802.11p [10], (3) SAE J2735 Dedicated Short Range Communications (DSRC) Message Set Dictionary [17], including the Basic Safety Messages (BSM) definition, and (4) the ETSI ITS specifications. In recent years, a cellular-based V2X technology called Cellular-V2X (C-V2X) has emerged as an alternative solution to IEEE 802.11p-based DSRC [15].

To improve overall road safety, BSM [17] and Cooperative Awareness Message (CAM) [6] aim to achieve the same goal – to share vehicle information, such as a vehicle's speed, position, acceleration in order to establish and maintain awareness of others vehicles nearby to improve road safety. The expected range of V2X communication is 300 to 500 m [18].

From a security and privacy perspective, IEEE 1609.2 [8] specifies the solution to make vehicular communication secure and protect the vehicle owners' privacy. The security architecture and solution in the ETSI ITS standard [4] are based on the IEEE 1609.2 [8] specification with modifications to adapt to the European market. The key part of the security solution in IEEE 1609.2 [8] is the use of digital certificates to verify the authenticity of vehicles and the validity of messages they transmit. Messages from transmitting vehicles include a message payload, a digital signature, and a digital certificate. Receiving vehicles use the public key in this digital certificate to confirm the message authenticity and integrity by verifying the digital signature on the message. In this sense, the essential part of the security solution in V2X communication is a PKI system that generates, distributes, and uses digital certificates.

Because of the periodic nature of BSM [17] and CAM [6] messages, they allow the use of certificate *digest*, a shorthand notation of a full certificate, to occasionally replace a full certificate in these messages. ETSI TS 103 097 [5] states that vehicles include a *digest* in CAM messages by default, and a certificate at most once per second. While this mechanism reduces the message overhead, it also creates a situation where receiving vehicles may not locally have the certificate that corresponds to a *digest*, and are thus unable to verify the received message. To resolve this situation, the standard provides a mechanism to query vehicles within communication range to provide the certificate for a given *digest*. Despite the perceived benefit of this mechanism, our simulation result indicates that its benefit is negligible. This is due to a large majority of the resolution of unknown certificates is for vehicles that only interact very briefly.

The rest of this paper is organized as follows. In Sec. II, we first describe the CAM transmission and reception as defined in the ETSI standard. Then in Sec. III, we discuss our simulation to recreate traffic flow based on real-world data and analyze its result. In Sec. IV, we evaluate the simulation and reflect its result to the existing standard. We discuss related work in Sec. V, and conclude the paper in Sec. VI.

This work was supported in part by CyberSecurity Research Flanders with reference number VR20192203 and by the Research Council KU Leuven C1 project on Security and Privacy for Cyber-Physical Systems and the Internet of Things with contract number C16/15/058.

978-1-6654-6975-3/22/$31.00 ©2022 IEEE

II. CAM Transmission and Reception

ETSI EN 302 637-2 [6] specifies CAM transmission and reception. In particular, it describes the criteria for vehicles to transmit CAM messages. Since the last CAM transmission, either[1]:

1) the direction change exceeds 4 degrees;
2) the distance change exceeds 4 meters; or
3) the speed change exceeds 0.5 meter/sec.

In addition, the minimum ($T\_GenCamMin$) and maximum transmission intervals ($T\_GenCamMax$) are 100 msec and 1 sec, respectively. In other words, vehicles transmit CAM messages at specific movement changes with the frequency of between 1 to 10 times per second. If the CAM transmission rate is higher than 1 message/sec, the vehicle includes a certificate in only one message per second.

As stated in Sec. I, the use of a certificate *digest* reduces the CAM message overhead. A study by C2C-CC indicates that the average CAM message size is 350 bytes while the size of certificates and signatures is between 100 bytes and 150 bytes [2]. This implies that the certificate and signature take up to 30% of the total message size. IEEE 1609.2 [8] defines this *digest* as `HashedId8` type which contains the least significant eight octets of the hash output of the certificate, ($d = LSB8(Hash(c))$, where d, $LSB8()$, $Hash()$, and c are a digest, a function to extract the least-significant eight octets of the argument, a cryptographic hash function, and a certificate, respectively). Thus, the use of *digest* reduces the certificate size from between 100 to 150 bytes to 8 bytes. This compact representation significantly reduces the total CAM message size. Because the CAM transmission is periodic and frequent, this reduction contributes to an efficient use of the radio channel.

On the other hand, the use of *digest* implies that receiving vehicles need to hold a mapping table that maps a *digest* to the corresponding certificate. This further implies that a situation can occur where a receiving vehicle does not have the certificate that maps to a *digest* received in a CAM message (*unknown certificate* situation). This situation occurs when a vehicle enters the communication range of another vehicle that just transmitted a CAM message with a *digest*. This is a problem as the receiving vehicle cannot verify the received CAM message due to the absence of a certificate. There are two approaches to resolve this situation. The first is to simply wait for the next CAM message containing the missing certificate. The second is to proactively request the missing certificate to be sent.

The IEEE 1609.2 [8] and EN 302 637-2 [6] specifications provide a mechanism to realize the latter approach. It is called *inlineP2pcdRequest* which was added to the IEEE 1609.2 amendment 1 [9]. In this mechanism, a receiving vehicle requests the missing certificate to be sent so that either the transmitting vehicle itself or any other vehicle within the communication range can respond by sending this certificate. This request uses a field in the CAM message header; the requesting vehicle populates one or more *unresolved digest(s)* in this header field to indicate that it requests the corresponding certificate(s) to be sent. Receiving vehicles of a CAM message containing an *inlineP2pcdRequest* in its header checks its local memory, and if it has the corresponding certificate, it sends a response message. IEEE 1609.2 defines a throttle mechanism to avoid an excessive number of responses by vehicles.

Minimizing delay in verifying received messages is an important factor in real-time cyber-physical systems such as V2X communication to avoid accidents and improve road safety. However, the *inlineP2pcdRequest* mechanism also increases the CAM message length and processing at both sending and receiving vehicles. An excessive processing burden in vehicles and communication channel congestion can also cause a delay in message verification. Furthermore, if the next CAM message containing a certificate arrives while *inlineP2pcdRequest* is in progress, this request becomes a futile effort. Given the $T\_GenCamMax$ value of 1 second, the next CAM message with a certificate is expected within 500 msec on average. Therefore, the time gap reduction for using this mechanism is an order of several 100 msec. A legitimate question is whether this is worth the effort. This paper investigates the benefit and effectiveness of this mechanism compared to the first *"do nothing"* approach in which the vehicle waits for the next CAM message containing the missing certificate.

III. Simulation to Reproduce Real-World Traffic Flow

To better understand the effectiveness of the *inlineP2pcdRequest* mechanism, we conducted a simulation to reproduce traffic flow based on real-world traffic data.

A. Traffic Data

We used the real-world traffic data from a government project conducted in 2019. This data contain vehicle flow in multi-lane highway segments and junctions that surround Antwerp, Belgium. The longest segment of collected data is approximately 9 km. The raw traffic data were recorded by inductive loops embedded in the road surface. The collected raw data include speed and size (length) of each passing vehicle over 24 hours a day for all lanes for one month. This log data provides insight into dynamic changes of traffic density over this entire collection period.

TABLE I: Vehicle Routes

Direction	Route	Label	From (position)	To (position)
Northbound	a	N-a	South entrance ①	East exit ②
Northbound	b	N-b	South entrance ①	North exit ③
Southbound	a	S-a	North entrance ③	South exit ①
Southbound	b	S-b	North entrance ③	East exit ②
Westbound	a	W-a	East entrance ②	North exit ③
Westbound	b	W-b	East entrance ②	South exit ①

The highway segment we consider is shown in Fig. 1 and in Table I; it consists of three directions (northbound,

[1]In addition to these, the 802.11p-based system requires an additional timer (T_GenCam_Dcc) defining the minimum interval between two consecutive CAM messages to prevent channel congestion.

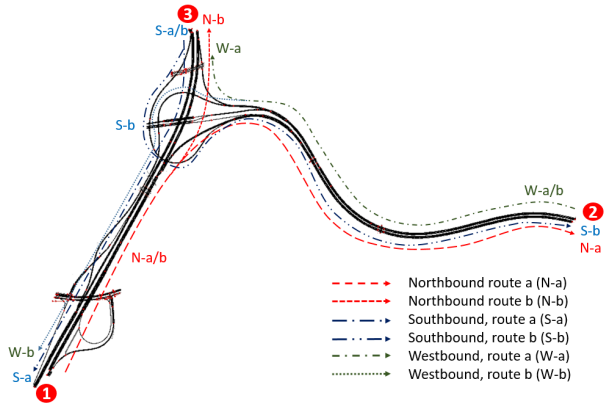
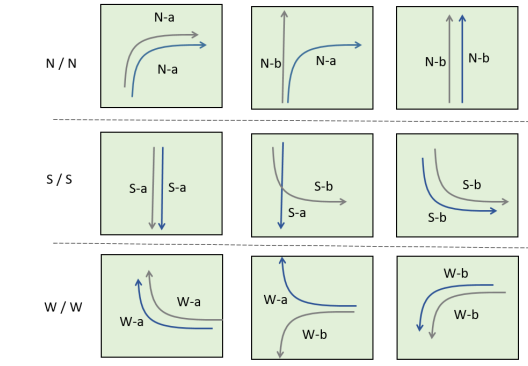
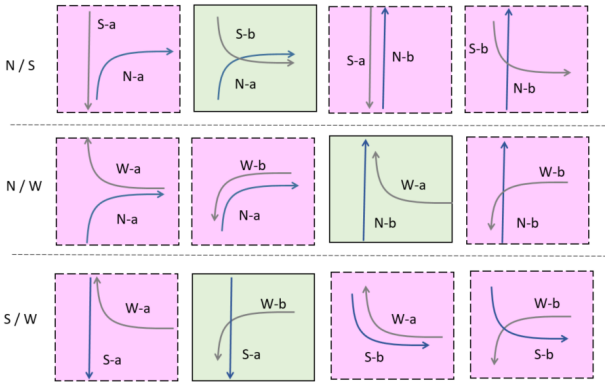


Fig. 1: Route of the Simulated Traffic



(a) Combination Group 1



(b) Combination Group 2

Fig. 2: Traffic Combinations

southbound, westbound) with each direction divided into two routes (a and b), for a total of 6 trajectories. We selected the busiest traffic day from the one-month period, and chose three one-hour time slots (high, medium, and low traffic density) from this day. Then we recreated the traffic flow of these three time slots using the SUMO traffic simulator [14].[2] We configured the SUMO simulator using the vehicle types and physical characteristics according to the definition from this national project: (1) passenger vehicle, (2) van, (3) lorrie, and (4) trailer and bus. We prepared 3 configuration files and ran the simulation 3 times to recreate high, medium, and low-density traffic according to the traffic density for each vehicle types as shown in Table II.

B. Approach and Methodology

We used the *vTypeProbe* output mode in SUMO to analyze the traffic flow. Output from this mode includes the latitude/longitude of each vehicle in 1 second increments. We used this data to calculate the distance between a given pair of vehicles. For each vehicle as a reference point, we calculated the distance change in every second to all other vehicles on the highway. With this distance data, we analyzed the traffic flow from the perspective of the reference vehicle entering and leaving the communication range of other vehicles. Then we repeated this process for all vehicles as the reference point. This way, we obtained a complete distance change history from all vehicles to all other vehicles during the course of their travel.

Next, we grouped the combinations of two trajectories and categorized them based on the perceived importance to resolve the *unknown certificate* condition. Figure 2 shows all possible combinations; among all 21 combinations, 9 of them fall into what we call *low-impact* category. These are shown in pink with a dotted-line boundary. This category is characterized by vehicles moving in opposite directions; they approach and move away from each other with minimal time spent in each other's communication range. The higher each other's relative

[2]Due to imported map data size limitation, the maximum highway segment in the SUMO simulation is limited to approx. 6km from the original data of approx. 9km segment.

TABLE II: Traffic Density (vehicles/hour)

Vehicle Type	Direction	Route	Traffic Density (High / Medium / Low)
Passenger	North	a	2887 / 2153 / 111
Passenger	North	b	2890 / 2157 / 112
Van	North	a	588 / 572 / 47
Van	North	b	591 / 575 / 49
Lorrie	North	a	95 / 171 / 30
Lorrie	North	b	98 / 173 / 32
Trailer, Bus	North	a	313 / 590 / 132
Trailer, Bus	North	b	314 / 591 / 133
Passenger	South	a	3110 / 2574 / 217
Passenger	South	b	1374 / 750 / 55
Van	South	a	1720 / 1612 / 69
Van	South	b	152 / 100 / 9
Lorrie	South	a	145 / 324 / 31
Lorrie	South	b	48 / 78 / 4
Trailer, Bus	South	a	278 / 598 / 108
Trailer, Bus	South	b	167 / 335 / 25
Passenger	West	a	2056 / 889 / 60
Passenger	West	b	2059 / 891 / 62
Van	West	a	196 / 153 / 17
Van	West	b	200 / 154 / 17
Lorrie	West	a	66 / 98 / 19
Lorrie	West	b	68 / 101 / 21
Trailer, Bus	West	a	164 / 399 / 69
Trailer, Bus	West	b	166 / 401 / 71

speed difference, such as in a highway scenario in our traffic data, the shorter this duration becomes. Once they leave the communication range, they are unlikely to meet again for the remainder of their trips. For example, two vehicles in opposite directions on a highway moving at 100 km/h spend only 5.4 to 9 seconds within each other's communication range of 300 to 500 meters. Using the *inlineP2pcdRequest* mechanism for such a short encounter does not appear to justify imposing additional processing in all vehicles within this communication range to resolve unknown certificates in broadcast CAM messages, given that the time saved is in the order of several 100 msec at best. The number of these requests increases proportionally to the traffic density, thus exacerbating the situation. Therefore we conclude the *inlineP2pcdRequest* mechanism in the *low-impact* category has the least benefit in highway scenarios. On the other hand, the remaining 12 combinations in Fig. 2 fall into the *high-impact* category, shown in green with a solid line boundary. All combinations in this category share the common characteristic that the inter-vehicle distance remains relatively stable for an extended period as they move in the same direction in whole or at least in part of their trajectories. Therefore, in this category, this mechanism is more beneficial.

Table III shows the resulting handling of the received CAM messages between two vehicles. Here "CR" (certificate request) indicates the receiving vehicle uses the *inlineP2pcdRequest* mechanism to resolve unknown certificates, while "ignore" means that the vehicle waits for the next CAM message with a certificate.

TABLE III: Unknown Certificate Handling Matrix

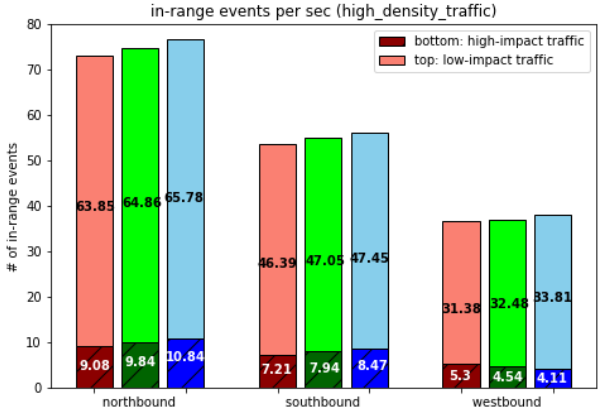
Direction-Route		Vehicle A					
		N-a	N-b	S-a	S-b	W-a	W-b
Vehicle B	N-a	CR	CR	ignore	CR	ignore	ignore
	N-b	–	CR	ignore	ignore	CR	ignore
	S-a	–	–	CR	CR	ignore	CR
	S-b	–	–	–	CR	ignore	ignore
	W-a	–	–	–	–	CR	CR
	W-b	–	–	–	–	–	CR

Note: CR: certificate request.

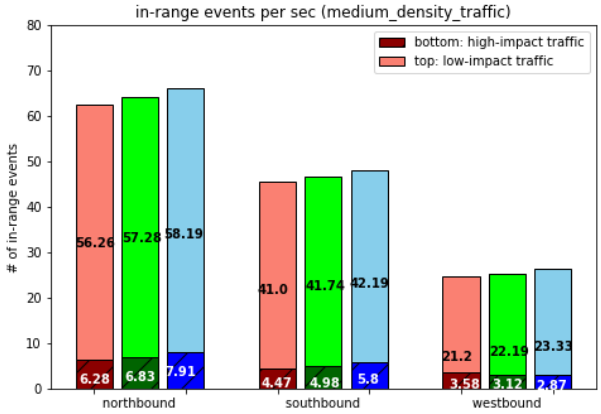
From the SUMO *vTypeProbe* output, we identified all events where a vehicle enters the communication range of another vehicle (we call it *in-range event* for the rest of this paper), applied the *high-* and *low-impact* categorization based on their trajectories, and counted the number of events in both categories. We analyzed the data using three communication range of 300 m, 400 m, and 500 m for all vehicle types and evaluated their effect. We selected these distances as they are the expected transmission range in both DSRC (ITS-G5) and C-V2X [18]. There are multiple criteria to trigger CAM messages as described in Sect. II. However, given that our data represents highway traffic, we use the vehicle speed to derive the transmission interval of vehicles to simplify our analysis.

IV. Discussion and Evaluation

Our analysis result is shown in Table IV and Fig. 3. Table IV shows the average duration a vehicle stays within the transmission range of another vehicle according to the traffic combination in Fig. 2. This duration is consistently longer for vehicles in the *high-impact* category and significantly shorter in the *low-impact* category. As discussed in Sec. III-B, this is intuitive as vehicles in opposite trajectories spend less time in each other's communication range than that of similar trajectories. Vehicles in the former category stay in their communication range between 2.3 to 6.6 times longer than the latter depending on this range.



(a) high-density traffic



(b) medium-density traffic

Fig. 3: In-Range Event per Second (The red, green, and blue bars represent the number of events per second in 300m, 400m, and 500m communication range, respectively. For each bar, the darker color at the bottom and the lighter color at the top show the *high-impact* and *low-impact* category.)

Figure 3(a) and 3(b) show the analysis of *in-range event* for high and medium density traffic, respectively[3]. In Fig. 3(a) and 3(b), *in-range events* are grouped based on traffic direction (north, south, westbound). In all cases, the number of *in-range*

[3]Low density traffic result is not shown as its numbers are significantly lower compared to these two scenarios, thus do not contribute additional value to the discussion.

TABLE IV: In-Range Duration (sec.)

Traffic Direction	Traffic Comb.	Comm. range: 300m			Comm. range: 400m			Comm. range: 500m		
		High-D	Med-D	Low-D	High-D	Med-D	Low-D	High-D	Med-D	Low-D
Northbound	High-Imp	72.19	72.77	61.50	79.20	79.29	68.37	83.89	83.61	73.26
	Low-Imp	15.15	14.87	12.94	19.78	19.44	16.57	24.46	24.07	20.14
Southbound	High-Imp	57.39	57.51	46.00	60.33	60.17	50.52	62.58	61.77	53.12
	Low-Imp	17.53	16.12	13.66	22.72	21.17	18.00	26.97	25.68	21.80
Westbound	High-Imp	88.09	89.15	73.17	99.30	101.05	84.75	107.23	107.56	90.91
	Low-Imp	13.69	13.51	12.37	18.13	17.82	16.81	23.44	23.09	21.21

Note: High-D: high-density, Med-D: medium-density, Low-D: low-density, High-Imp: high-impact, Low-Imp: low-impact.

events for the *low-impact* category are significantly higher than that of the *high-impact* category. On average, high-density traffic indicates that 85.6% to 89.2% of all *in-range events* occur between vehicles in the *low-impact* category. In medium-density traffic, this value is slightly higher between 85.5% to 90.0%. This trend is consistent across all communication distance of 300m, 400m, and 500m. In other words, a large majority of *in-range events* occur with vehicles in the *low-impact* category, and the events with vehicles in the *high-impact* category are a minority. Again, this result reflects our intuition – the *in-range event* occurs more frequently with relatively high speed difference between two vehicles, such as vehicles in opposing directions. On the other hand, vehicles moving in the same or similar trajectory have lower relative speed difference. Thus, threshold-cross events occur less often.

If we suppress the *inlineP2pcdRequest* mechanism in all *low-impact* category vehicles, it reduces a large proportion of such events. There are a number of benefits of doing so: it (1) reduces the processing and transmission of *inlineP2pcdRequest* in the CAM header from the requesting vehicle, (2) relieves the processing of these requests in all other vehicles within the communication range, and (3) reduces the use of communication channel.

Table V summarizes the resulting improvement due to suppressing the *inlineP2pcdRequest* for *low-impact* category. Our simulation result indicates that the minimum and the maximum number of CAM messages/sec is 4.28 to 6.21 in high- and medium-density traffic.[4] As we described in Sec. II, the CAM messages periodically include a full certificate at every 1 second interval. This implies that the probability of an *unknown certificate* situation is 76.6% to 83.9% of all *in-range events*. If we include the *inlineP2pcdRequest* in the CAM message header for all such events, as specified in IEEE 1609.2 [8], there are 58.69 and 55.46 requests per second for high- and medium-density traffic. If we suppress all these requests for *in-range events* in the *low-impact* category, then based on the number in Fig. 3(a) and 3(b), the average number of CAM messages containing the *inlineP2pcdRequest* reduces to 8.30 and 6.64 requests/sec, respectively. This is a 7.1 to 8.4 times improvement over the default behavior of generating *inlineP2pcdRequest* without considering the traffic trajectory.

We acknowledge that our scheme relies on unverified CAM messages due to the absence of a certificate in received messages. In this sense, we assume an *honest majority*, i.e. a large proportion of the vehicles are honest and send genuine information in their CAM messages. Such an assumption may be a concern. However, it has only a negligible implication. If we ignore all *unknown certificate* situations irrespective of vehicle trajectories, we fall back to the *"do nothing"* approach and simply wait for the next CAM message with a certificate attached. If no such message is received from a given vehicle, it means that this vehicle has likely moved out of the communication range already. Thus we can safely disregard this vehicle. We also note that this simulation result and evaluation are limited to the highway traffic environment. Thus, we may obtain a different view in other environments such as busy local streets. However, our analysis indicates that using the *inlineP2pcdRequest* mechanism has almost no benefit in the highway environment while it only incurs additional processing in vehicles. Therefore, we conclude that vehicles should apply the *inlineP2pcdRequest* mechanism based on its attributes, such as speed, relative to that of encountered vehicles. This way, vehicles can use this mechanism where it is truly beneficial.

[4]The CAM messages/sec is lower in high density traffic due to relatively lower speed than medium density traffic.

TABLE V: Reduced Overhead Due to InlineP2pcdRequest Message Supression

Data Points	Traffic density	
	High	Medium
# of CAM messages/sec	4.28	6.21
in-range events/sec	76.62	66.10
% of "unknown cert." condition	76.6%	83.9%
inlineP2pcdRequest events/sec (default)	58.69	55.46
high-impact %	14.14%	11.97%
inlineP2pcdRequest events (improved)	8.30	6.64

V. Related Work

Several works of literature discuss the impact of security-related processing in V2X communication and mention digest use in CAM messages. Javed et al. [11] and Brahim et al. [1] investigated the impact of processing ECC-based signature and encryption algorithm and evaluated their performance. Muhammad et al. [15] measured and analyzed the security overhead in broadcast communication in LTE C-V2X from the integrity and authenticity protection processing perspective. From a V2X-based service perspective, Lonc and Cincilla [13]

summarize the implementation status of security services as defined in the ETSI ITS standard, and Labiod et al. [12] propose a service advertisement message called CAM-I.

All these studies mention certificate *digest* in CAM messages as background information within the context of their discussion. From a performance perspective, the common conclusion is that the overhead in security processing in C-ITS results in additional delay [1], [11], [15]. As such, they only mention the certificate *digest* as a feature in the ETSI ITS standard to reduce message size; no consideration is given to its usefulness in traffic patterns as we focus in this paper. To the best of our knowledge, the usefulness and the issue related to resolving unknown certificates in CAM messages using the *inlineP2pcdRequest* mechanism has not been studied.

VI. Conclusion and Future Work

We presented the simulation result and analysis of using the *inlineP2pcdRequest* mechanism in highway scenario based on real-world traffic data. Based on our findings, we conclude that this mechanism has more disadvantages than advantages; it only increases processing loads in vehicles and the higher utilization of communication channel while its benefits remain unclear. Therefore, we propose ETSI and IEEE reevaluate this mechanism in their standards and modify its specification. Furthermore, conducting field test and measuring the message processing overhead of this mechanism on a hardware platform will further reinforce our understanding of the performance implications. Also, additional simulation and analysis using other types of traffic scenarios would complement our findings further to understand this mechanism's benefits. We consider these areas our next step.

Acknowledgment

We express our gratitude to Be-Mobile NV, Prof. Chris Tampére and Dr. Mohammad Ali Arman of the Mechanical Engineering Dept. in KU Leuven for providing the traffic data. We also thank Dr. Dave Singelée in COSIC group in KU Leuven, Dr. Xavier Carpent and Ms. Dimah Mohammed Almani in Computer Science Dept. in Univ. of Nottingham for their insights.

References

[1] M. B. Brahim, E. B. Hamida, F. Filali and N. Hamdi, "Performance impact of security on cooperative awareness in dense urban vehicular networks", *2015 IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, IEEE, pp. 268–274, 2015

[2] Car 2 Car Communication Consortium (C2C-CC) TR2052, "Survey on ITS-G5 CAM Statistics", [Online]: https://www.car-2-car.org/documents/general-documents/, Dec. 2018

[3] EU project Concorda [Online]: https://ertico.com/concorda/

[4] European Telecommunication Standard Institute (ETSI), *TS 102 940 Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management*, Ver.2.1.1, July 2018.

[5] European Telecommunication Standard Institute (ETSI), *TS 103 097 Intelligent Transport Systems (ITS); Security; Security header and certificate formats; Release 2*, Ver.2.1.1, Oct. 2021.

[6] European Telecommunication Standard Institute (ETSI), "EN 302637-2 Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service," Ver.1.4.1, Apr. 2019.

[7] N. Huq, C. Gibson, R. Vosseler, "Driving Security Into Connected Cars: Threat Model and Recommendations", Trend Micro Inc., 2020

[8] IEEE Vehicular Technology Society, "IEEE Standard for Wireless Access in Vehicular Environments—Security Services for Applications and Management Messages," IEEE Std 1609.2-2016, 2016

[9] IEEE Vehicular Technology Society, "IEEE Standard for Wireless Access in Vehicular Environments—Security Services for Applications and Management Messages Amendment 1," IEEE Std 1609.2a-2017, 2017

[10] IEEE Computer Society, *IEEE Standard for Information technology - Telecommunication and information exchange between systems - Local and metropolitan area networks - Specific requirements Part11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment6: Wireless Access in Vehicular Environments*, IEEE Std. 802.11p-2010

[11] M. A. Javed, E. Ben Hamida and W. Znaidi, "Security in intelligent transport systems for smart cities: From theory to practice", *Sensors Journal*, MDPI, Vol. 16, No. 6, pp. 879–903, 2016

[12] H. Labiod, A. Servel, G. Seggara, B. Hammi and J. P. Monteuuis, "A new service advertisement message for ETSI ITS environments: CAM-Infrastructure", *2016 8th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, IEEE, pp. 1–4, 2016

[13] B. Lonc and P. Cincilla, "Cooperative its security framework: Standards and implementations progress in Europe", *2016 IEEE 17th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, pp. 1–6, IEEE, 2016

[14] P. A. Lopez, M. Behrisch, L. Bieker-Walz, J. Erdmann, Y-P Flötteröd, R. Hilbrich, L. Lücken, J. Rummel, P. Wagner and E. Wießner, "Microscopic Traffic Simulation using SUMO", The 21st IEEE International Conference on Intelligent Transportation Systems, *IEEE Intelligent Transportation Systems Conference (ITSC)*, IEEE, [Online]: https://elib.dlr.de/124092/

[15] M. Muhammad, P. Kearney, A. Aneiba and A. Kunz, "Analysis of security overhead in broadcast V2V communications", *International Conference on Computer Safety, Reliability, and Security*, pp. 251–263, Springer, 2019

[16] M. Renner, N. Münzenberger, J. von Hammerstein, S. Lins and A. Sunyaev, "Challenges of Vehicle-to-Everything Communication. Interviews among Industry Experts", Wirtschaftsinformatik (Zentrale Tracks), pp. 1831–1843, 2020

[17] SAE International, *Surface Vehicle Standard, V2X Communications Message Set Dictionary*, SAE Int'l. J2735-2006

[18] B. Stojanović and K. Hofer-Schmitz, "Formal Methods for Connected Vehicle Protocols", *2019 27th Telecommunications Forum (TELFOR)*, pp. 1–4, IEEE, 2019

[19] D. Yang, K. Jiang, D. Zhao, C. Yu, Z. Cao, S. Xie, Z. Xiao, X. Jiao, S. Wang and K. Zhang, "Intelligent and connected vehicles: Current status and future perspectives", *Science China Technological Sciences*, vol. 61, no. 10, pp. 1446–1471, Springer, 2018