Efficient Rate-Adaptive Certificate Distribution in VANETs

Sebastian Bittl, Berke Aydinli, Karsten Roscher
Fraunhofer ESK
Munich, Germany
{sebastian.bittl,berke.aydinli,karsten.roscher}@esk.fraunhofer.de

***Abstract*—Car-to-X communication systems, often called vehicular ad-hoc networks (VANETs), are in the process of entering the mass market in upcoming years. Thereby, security is a core point of concern due to the intended use for safety critical driver assistance systems. However, currently suggested security mechanisms introduce significant overhead into Car-to-X systems in terms of channel load and delay. Especially, the usage of on the fly distributed pseudonym certificates leads to a trade off between channel load and authentication delay, which may lead to significant packet loss. Thus, this work studies a novel concept for pseudonym certificate distribution in VANETs using rate-adaptive certificate distribution based on monitoring a vehicle's environment. Thereby, the cyclic certificate emission frequency is adapted on the fly based on cooperative awareness metrics for discrete parts of the vehicle's surrounding. The obtained mechanism is evaluated in a highway as well as an urban simulation scenario to show its suitability for a broad range of traffic conditions. Thereby, we find that it is able to significantly outperform the currently standardized approach for pseudonym certificate distribution in VANETs based on ETSI ITS standards. Thus, it should be regarded for further development of future VANETs.**

I. Introduction

Vehicular ad-hoc networks (VANETs) are about to enter the mass market in upcoming years. Thereby, current standardization efforts include ETSI Intelligent Transport Systems (ITS) in Europe [1] and Wireless Access in Vehicular Environments (WAVE) in the USA [2]. Both systems use a single wireless control channel for safety critical message exchange between nodes (often called ITS-stations (ITS-S)). Future safety critical advanced driver assistance systems (ADAS) are intended to be based on the exchanged information sets. Thus, efficient security mechanisms are required to allow for reliable communication between ITS-Ss.

The security system of VANETs is typically based on a digital signature scheme supported by so-called pseudonym certificates. These are changed by each ITS-S rapidly to avoid tracking. This system requires the exchange of certificates between stations prior to actual communication of vehicle information used by ADAS. Instead of using dedicated messages for certificate exchange, these data sets are piggybacked in the so-called security envelope of periodically distributed messages. Cooperative Awareness Messages (CAMs) are used for such basic information exchange in ETSI ITS [3].

However, such certificate distribution has been found to cause significant overhead on the highly bandwidth restricted single control channel [4]–[6]. Thereby, it was found that the security overhead regarding message size significantly exceeds the length of real payload for standard ETSI ITS messages. Moreover, the biggest share of this overhead is caused by included certificates [5], [6]. Thus, the need for strategies to distribute the certificates only in a subset of all sent messages has been discovered [7].

Prior work has studied different concepts of certificate distribution in VANETs, like cyclic, neighborhood aware or congestion based certificate distribution [5], [8], [9]. The current ETSI ITS standard [10] specifies usage of a combination of different approaches. A study on their parametrization showed the influence of separate sub-mechanisms on overall system performance [11]. The parametrization yielding best performance, according to the results in [11], is used as a reference system in this work. However, prior studies have focused on fixed inclusion frequencies for cyclic certificate emission. This basic mechanism is combined with different approaches for additional certificate emission [10] or suppression of dedicated certificate emissions [9].

In contrast, this work introduces the concept of an adaptive inclusion frequency of pseudonym certificates. Thereby, we use the idea of areas with different awareness requirements introduced in [9], to obtain a metric for live feedback from a station's surrounding. This metric is used to adjust the inclusion frequency on demand.

The remainder of this work is structured as follows. Related work is studied in Section II. Section III introduces the novel rate-adaptive certificate distribution scheme. An evaluation of the algorithm is provided in Section IV. Finally, a conclusion is given in Section V together with topics of future work.

II. Related Work

Prior work regarding pseudonym certificate distribution in VANETs can be found, e.g., in [4], [5], [7]–[10]. Thereby, certificates are distributed by piggybacking them onto the facility layer messages. In order to save bandwidth on the single ETSI ITS control channel [12], at first basic certificate emission mechanisms like pure cyclic inclusion or detection of new neighbors were considered [7], [8]. The importance of using such message shortening strategies has been shown in [4], [8], as the additional overhead caused by the security envelope, which among other data contains the certificate, leads to significantly increased channel load. Thereby, the

amount of packet collisions is increased and the average communication distance of vehicles decreases, both leading to worse cooperative awareness.

Current ETSI ITS standards specify usage of a combination of a multitude of different certificate distribution mechanisms [10]. These include cyclic, neighborhood-based and request-based certificate emission. Thereby, the neighborhood-based scheme can be regarded as an indirect request scheme, which can speed up certificate distribution significantly reducing so-called cryptographic packet loss, i.e., discarding of received messages as they could not be verified [11].

Congestion-based certificate emission for traffic scenarios leading to a highly congested wireless channel is studied in [5], [9]. We do not target this kind of scenarios in the following, but the basic concept of using separated zones of interest in a vehicle's surrounding, developed in [5], [9], is reused in this work. However, we do not only use it for evaluation purposes, but also as live feedback inside communicating ITS-S to adjust the certificate emission rate on demand.

Different metrics for determining the performance of VANETs have been suggested. A recent promising approach for safety critical applications is to use the cooperative awareness quality of nodes, which was originally proposed in [13]. This metric is mainly used in [5], [9] to determine the impact of certificate emission on overall VANET performance.

III. Rate-Adaptive Certificate Distribution

Our adaptive pseudonym certificate distribution scheme is built on top of the standardized mechanisms from [10] and their parametrization studied in detail in [11]. Thus, we use implicit as well as explicit certificate requests alongside with cyclic certificate emission. However, we vary the distribution algorithm from [10] in regard to the following major points.

1) Position-based weighting of the significance of a request. In prior work all requests are weighted equally.
2) Adaption of the certificate inclusion frequency based on current weights of received requests.

The significance of a request is determined by assigning its sender to one of four relevance areas based on its current location relative to the location of the receiver. This concept is illustrated in Figure 1. The discretization of a vehicle's surrounding is inspired by the evaluation concept used in [5], [9]. However, while [5], [9] use this concept just for off-line evaluation with global knowledge about the whole network (i.e., ground truth), we use these areas for on-line calculation of a metric describing a vehicle's environment at different distances. Moreover, we adapt the size of the relevance areas based on the current communication conditions, while work in references [5], [9] uses areas of a-priori fixed size.

Communication conditions change based on the current traffic scenario in which an ITS-S participates. Thus, the distance at which reliable communication is possible also changes alongside with the traffic conditions. Our assumption is that it is more important to ensure authentication of other ITS-Ss which have a higher probability for good communication conditions, i.e., ITS-Ss which are close to the own ITS-S, in comparison to those being more far away, which also means higher average outage probability. Furthermore, closer ITS-Ss are typically more relevant for safety critical ADAS, e.g., for collision avoidance.

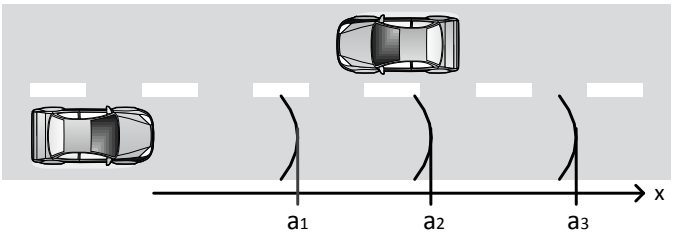

Fig. 1. Regions of interest in a vehicle's surrounding.

Moreover, we assume communication conditions between ITS-Ss to be symmetric. Thus, possibility of a bidirectional communication is assumed after successful unidirectional one.

The boundaries a_i ($i \in [1;4]$) of the individual areas A_i are given by Equations 1 to 4.

$$a_1 = \frac{1}{N}\sum_{j=1}^{N} d_j \tag{1}$$

$$a_3 = \max d_j; j \in [1;N] \tag{2}$$

$$a_2 = \frac{a_1 + a_3}{2} \tag{3}$$

$$a_4 = \infty \tag{4}$$

Thereby, the number of currently known nodes in a ITS-S's surrounding is given by N and the distance of the own ITS-S to another ITS-S j is denoted by d_j. An ITS-S gets removed from the list of known nodes after no message has been received for a time span superseding a certain timeout limit. A limit of two seconds is used in the following, which corresponds to the double of the maximum transmission interval of CAMs. This means that the algorithm tolerates missing at least one CAM from other ITS-S without removing them from the list of known ITS-S. The fourth area is used to filter requests from ITS-Ss, which are so far away that no stable (reliable) communication connection with them is possible, i.e., only sporadic message exchange is possible.

After a received request has been assigned to a relevance area A_i, the current authentication ratio r_i inside A_i is calculated by

$$r_i = \frac{n_{i,auth}}{n_{i,known}};\ n_{i,auth} \leq n_{i,known};\ r_i \in [0;1]\,. \tag{5}$$

With $n_{i,auth}$ giving the number of nodes within A_i whose certificate is known and verified (i.e., these nodes are authenticated) and $n_{i,known}$ being the number of all nodes from whom messages have been received.

The individual authentication ratios r_i are combined to a unified weighted authentication ratio r_w by

$$r_w = \sum_{i=1}^{3} w_i \cdot r_i;\ \ \sum_{i=1}^{3} w_i = 1;\ w_i \geq 0. \tag{6}$$

This also means that the authentication ratio within A_4 is ignored for determining the certificate emission frequency.

The time period p_{cert} between two successive certificate emissions is determined via

$$p_{cert} = \max\left[\left(\frac{r_w}{1-r_w}\right)^z \cdot 0.1\text{s}; p_{cert,min}\right]. \quad (7)$$

Therefore, the certificate inclusion frequency f_{cert} is given by $f_{cert} = p_{cert}^{-1}$. In case of $r_w = 1$ cyclic inclusion of certificates is turned off. The minimum value of p_{cert} ($p_{cert,min}$) is given by the minimum delay between successive sending of two CAMs. The lower limit for $p_{cert,min}$ ($\min(p_{cert,min})$) is given by the 10 Hz maximum CAM emission frequency, i.e., a period of $\min(p_{cert,min}) = 0.1$s. This determines the maximum certificate emission frequency, as the security entity cannot trigger the sending of messages on its own, but relies on piggybacking its data to messages generated at higher protocol layers (e.g., CAMs). The parameter z is used to adjust the reactivity of the algorithm against changes in the monitored weighted authentication ratio in its surrounding.

The influence of z on the inclusion period of certificates is shown in Figure 2 for the case of a CAM emission frequency of 10 Hz ($p_{cert,min} = 0.1$s).

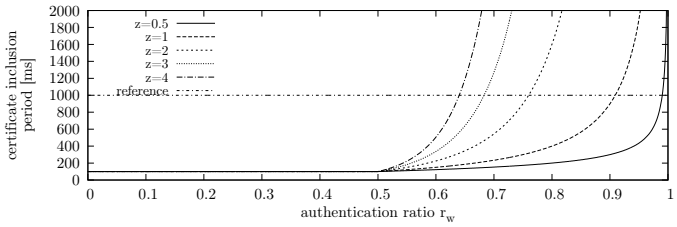

Fig. 2. Influence of the exponent z on certificate inclusion period.

One can clearly see from Equation 7 and Figure 2 that for $r_w = 1$ cyclic certificate emission is turned off totally. This corresponds to a traffic scenario in which the surrounding of a vehicle does not change over time, e.g., inside a large scale traffic jam. Clearly, there is no need for certificate emission in such kind of scenarios as all vehicles already know about the certificates of vehicles within their communication range.

As one can see from Figure 2, decreasing values of z lead to increased changes of p_{cert} alongside changes in r_w. Thus, reaction of the certificate emission algorithm on detected changes in the vehicle's surrounding is faster for lower values of z. However, this can also lead to an overreaction, as it takes time until feedback (in the form of a CAM with included certificate) arrives from the station(s) causing $r_w \neq 1$. During that time span unnecessary certificate emissions may occur due to a too large reduction in p_{cert} for high values of z. This shows the need to consider the trade-off between channel load and cryptographic packet loss, i.e., discarded received packets due to not available certificates for verification.

The reference value shown in Figure 2 is the fixed cyclic certificate inclusion period of 1s from [10]. One can clearly see that the adaptive scheme uses a significantly longer inclusion period for high values of r_w, which can be expected to lower channel utilization within well known surroundings.

One should note that according to the current standard for the security envelope, CAMs are not tagged with a location stamp by the security entity of the protocol stack. However, this information is available in a required data field of a CAM [3], [10]. Thus, our implementation looks into the secured data to obtain this information. This is not required for BSMs in the WAVE system, as the security envelope of these kind of messages contains a location stamp [14].

One could also think of using a weighting function for a request's significance which calculates the weight of a vehicle's request directly from the distance to the receiving vehicle, e.g., by a linear dependence. However, we decided for the discretization approach due to its higher robustness, e.g., against vehicle position jumps due to GPS inaccuracy (especially in urban scenarios).

An evaluation for the suggested certificate distribution scheme is provided in the following Section IV.

IV. Evaluation

In order to evaluate our approach to the certificate distribution problem from Section III before, we use the simulation environment discussed in Section IV-A. It is parametrized with the scenarios given in Section IV-B. Thereby, the performance metrics discussed in Section IV-C are determined. Obtained results are provided and discussed in Section IV-D. Moreover, the standardized certificate distribution mechanism from [10] is parametrized with the findings from [11] to ensure best performance for this reference scheme.

A. Simulation Environment

The used simulation environment consists of three major parts. Thereby, a fully ETSI ITS compatible Car-to-X protocol stack is provided by the ezCar2X framework. This stack is embedded into the network simulator ns-3 [15], which is used for simulating access and physical layer behaviors. Vehicle movement is provided by the microscopic traffic flow simulator SUMO [16] that is connected to its ns-3 counterpart via the so-called TraCI interface. A detailed description of the simulation environment can be found in [17].

B. Scenarios

We use two different scenarios to evaluate our approach. At first, the well known highway scenario with deterministic traffic flows on all six lanes (three in each direction) is studied. Thereby, intervals and speeds of vehicles on different lanes are adjusted as given in [18].

The second considered scenario resembles a real world urban roundabout. It was built up by exporting a roundabout found in Munich Maxvorstadt from Open Street Map (OSM). The obtained network was imported into SUMO. Traffic flows were generated from the SUMO random trip generator. To ensure statistically significant results, the simulation was run multiple times with different inputs for the initial random seed.

For both considered scenarios the so-called core zone concept [18], [19] was applied to avoid edge effects. This means,

statistical values are only assembled inside a geographical subset of the whole simulation area, which is surrounded by extra simulated area.

C. Performance Metrics

We study two metrics for the performance of pseudonym certificate distribution in VANETs. These are

1) number of certificate emissions per second as a metric for the channel load caused by each station and
2) cooperative awareness as defined in [5].

Thereby, the cooperative awareness metric (called awareness quality over time (AQT) in [5]) tries to summarize overall system performance. This includes the trade off between authentication delay via cryptographic packet loss and channel load. Basically, AQT gives the time weighted ratio between authenticated vehicles in a certain area A_i and the overall number of vehicles inside this area (ground truth).

However, while cooperative awareness tries to summarize the whole system performance, it only takes into regard whether the available wireless channel allows to use the applications which are actually in use. This means especially, it does not take into regard whether the system has still some spare resources for further applications or not.

The basic channel load in VANETs is typically built up by cyclic status messages of the individual nodes (CAMs in ETSI ITS and BSMs in WAVE) as they are used in our simulated scenarios. However, there has to be some spare capacity left for on demand distributed event messages, e.g., Decentralized Environment Notification Messages (DENMs) in ETSI ITS. Thus, we also study the channel load caused by each ITS-S by emitting its certificate. In case of two communication configurations which achieve the same level of cooperative awareness, the system causing less channel load should be preferred to leave as much as possible spare channel capacity for other applications.

D. Results

At first, results for cooperative awareness quality in both traffic scenarios from Section IV-B are given. Achieved results for the certificate emission rate are discussed later on.

Figure 3 gives the obtained cooperative awareness for different traffic densities in the freeway scenario. One can see that for this scenario with high node mobility, the standardized certificate distribution mechanism (denoted by *standard*) only slightly outperforms the new strategy from Section III for low traffic densities (denoted by *adaptive*). For vehicle intervals smaller then 6s the standard strategy is always outperformed by the adaptive strategy.

This finding of good performance of the adaptive strategy is also found in the roundabout scenario, as illustrated in Figure 4. For this scenario, the adaptive strategy always significantly outperforms its standardized counterpart. Thereby, the biggest gain occurs for the lowest considered traffic density.

These results show, that the adaptive strategy is able to improve cooperative awareness quality for most of the considered traffic scenarios. Thus, higher level applications can

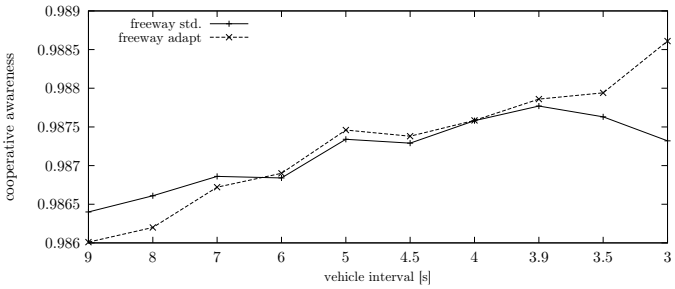

Fig. 3. Cooperative awareness within A_1 to A_3 for the freeway scenario.

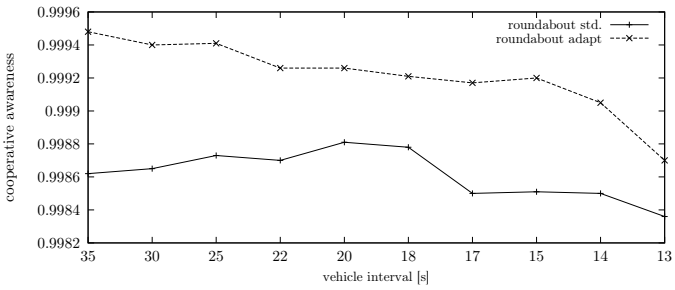

Fig. 4. Cooperative awareness within A_1 to A_3 for the roundabout scenario.

be expected to profit from a shift to the new approach by an increased quality of the database they operate on.

The second regarded performance metric is the average emission rate of pseudonym certificates (i.e., number of certificate emissions per second). The lower bound for this value for the standard strategy is one, as the standard specifies a fixed cyclic certificate inclusion frequency of 1 Hz [10]. Obtained results for this metric for the freeway scenario are given in Figure 5. One can clearly see, that the adaptive scheme

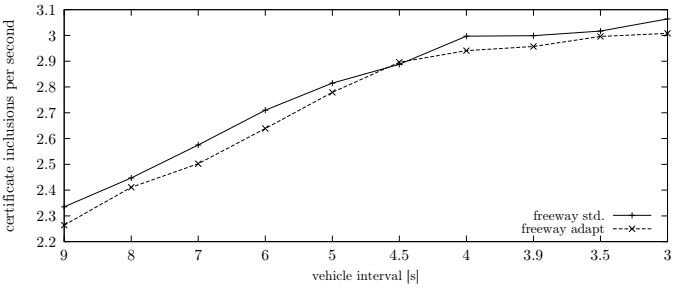

Fig. 5. Average number of certificate emissions per second by a single ITS-S in the freeway scenario.

yields lower certificate emission rates for all considered traffic densities. This means that the security overhead's impact on channel load caused by this scheme is lower than the one of the standard certificate distribution mechanism.

Finally, the results for the certificate emission rate for the roundabout scenario are provided in Figure 6. As for the freeway scenario (see also Figure 5 before), the adaptive distribution scheme achieves a lower certificate emission rate than its standardized counterpart. Moreover, the gain is more significant in the roundabout scenario in comparison to the

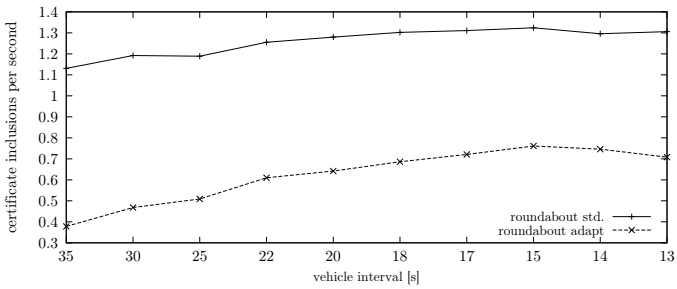

Fig. 6. Average number of certificate emissions per second by a single ITS-S in the roundabout scenario.

freeway scenario, especially for low traffic densities.

The reason for this finding can be assumed to be the fixed certificate emission frequency of 1 Hz in the standardized scheme. This frequency is higher than necessary to achieve high cooperative awareness and the additional emissions are not able to significantly increase cooperative awareness over the level which can be reached by much lower distribution frequencies, as they are used by the adaptive scheme (see also Figure 4 above). Thus, the additional certificate emissions can be regarded as pure overhead. The adaptive scheme is clearly able to significantly limit this overhead in comparison to the standardized scheme.

A conclusion about the results obtained in this work is provided in the following Section V.

V. Conclusion and Future Work

In the wake of upcoming deployment, the security mechanisms of VANET approaches are a core point of concern. The distribution of used pseudonym certificates carrying required security configuration parameters, e.g., public keys, introduces a major source of overhead into VANETs. Multiple approaches to achieve a well usable trade off between increased channel utilization and delayed communication by authentication delay have been suggested.

We have proposed a novel mechanism for on demand control of certificate distribution, which uses an adaptive model of a vehicle's surrounding. This model is based on discrete zones of required cooperative awareness quality. The weighting of the metrics for the different zones allows to prioritize reaction to newly discovered vehicles, for example to react quicker to closer vehicles than to ones more far away.

In our simulation-based evaluation, we show that the new approach can significantly outperform the currently standardized approach. Especially, in the urban roundabout scenario the traffic load caused by individual vehicles' certificate distribution can be reduced while cooperative awareness is even increased at the same time. In the freeway scenario the gain is smaller, but still the adaptive scheme can be regarded as a well usable alternative to the standardized mechanisms. Thus, we consider the suggested approach to be well usable in the development of future VANET systems.

Future work can study mechanisms to make the prioritization process of vehicles with unknown certificates more need driven by used applications. For example, active applications may not be interested in data from vehicles traveling on roads being parallel the currently used one.

References

[1] "Memorandum of Understanding for OEMs within the CAR 2 CAR Communication Consortium on Deployment Strategy for cooperative ITS in Europe," June 2011, v 4.0102.

[2] J. Harding, G. R. Powell, R. F. Yoon, J., C. Doyle, D. Sade, M. Lukuc, J. Simons, and J. Wang, "Vehicle-to-Vehicle Communications: Readiness of V2V Technology for Application," Washington, DC: National Highway Traffic Safety Administration, Tech. Rep. DOT HS 812 014, Aug. 2014.

[3] *Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service*, ETSI ES 302 637-2, Rev. V1.3.0, Aug. 2013,

[4] G. Calandriello, P. Papadimitratos, J. P. Hubaux, and A. Lioy, "On the Performance of Secure Vehicular Communication Systems," *IEEE Transactions on Dependable and Secure Computing*, vol. 8, no. 6, pp. 898 – 912, Sept. 2011.

[5] M. Feiri, J. Petit, R. Schmidt, and F. Kargl, "The Impact of Security on Cooperative Awareness in VANET," in *IEEE Vehicular Networking Conference*, Dec. 2013, pp. 127 – 134.

[6] S. Bittl, A. A. Gonzalez, and W. Heidrich, "Performance Comparision of Encoding Schemes for ETSI ITS C2X Communication Systems," in *Third International Conference on Advances in Vehicular Systems, Technologies and Applications*, June 2014, pp. 58–63.

[7] F. Kargl, E. Schoch, B. Wiedersheim, and T. Leinmüller, "Secure and Efficient Beaconing for Vehicular Networks," in *Proceedings of the fifth ACM international workshop on VehiculAr Inter-NETworking*, 2008, pp. 82–83.

[8] E. Schoch and F. Kargl, "On the Efficientcy of Secure Beaconing in VANETs," in *Proceedings of the Third ACM Conference on Wireless Network Security*, 2010, pp. 111 – 116.

[9] M. Feiri, J. Petit, and F. Kargl, "Evaluation of Congestion-based Certificate Omission in VANETs," in *IEEE Vehicular Networking Conference*, Nov. 2012, pp. 101 – 108.

[10] *Intelligent Transport Systems (ITS); Security; Security header and certificate formats*, ETSI TS 103 097, Rev. V1.1.1, 2013.

[11] S. Bittl, B. Aydinli, and K. Roscher, "Effective Certificate Distribution in ETSI ITS VANETs using Implicit and Explicit Requests," in *8th International Workshop Nets4Cars/Nets4Trains/Nets4Aircraft*, ser. LNCS 9066, M. Kassab et al., Ed., May 2015, pp. 72–83.

[12] *Intelligent Transport Systems (ITS); European profile standard for the physical and medium access control layer of Intelligent Transport Systems operating in the 5 GHz frequency band*, ETSI European Standard 202 663, Rev. V1.1.0.

[13] R. Schmidt, R. Lasowski, T. Leinmüller, C. Linhoff-Popien, and G. Schafer, "An Approach for Selective Beacon Forwarding to Improve Cooperative Awareness," in *IEEE Vehicular Networking Conference (VNC)*, 2010, pp. 182–188.

[14] *Draft Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages*, Intelligent Transportation Systems Commitee of the IEEE Vehicular Technology Society Std. P1609.2, Rev. D12, Jan. 2012, P1609.2, D12.

[15] G. F. Riley and T. R. Henderson, "The ns-3 Network Simulator," in *Modeling and Tools for Network Simulation*, K. Wehrle, M. Günes, and J. Gross, Eds. Springer Berlin Heidelberg, 2010, pp. 15–34.

[16] M. Behrisch, L. Bieker, J. Erdmann, and D. Krajzewicz, "SUMO - Simulation of Urban MObility: An Overview," in *The Third International Conference on Advances in System Simulation*, Oct. 2011, pp. 63–68.

[17] K. Roscher, S. Bittl, A. A. Gonzalez, M. Myrtus, and J. Jiru, "ezCar2X: Rapid-Prototyping of Communication Technologies and Cooperative ITS Applications on Real Targets and Inside Simulation Environments," in *11th Conference Wireless Communication and Information*, Oct. 2014, pp. 51 – 62.

[18] *Intelligent Transport Systems (ITS); STDMA recommended parameters and settings for cooperative ITS; Access Layer Part*, ETSI TR 102 861, Rev. V1.1.1, 2012, v1.1.1.

[19] Kloiber, B., Strang, T., de Ponte-Mueller, F. et al., "An Approach for Performance Analysis of ETSI ITS-G5A MAC for Safety Applications," in *ITST*, Nov. 2010.