Efficient Distribution of Static or Slowly Changing Configuration Parameters in VANETs

Sebastian Bittl
Fraunhofer ESK
Munich, Germany
sebastian.bittl@esk.fraunhofer.de

***Abstract*—Vehicular ad hoc networks (VANETs) based on Car2X communication technologies are about to enter mass production in the next years. Thereby, bandwidth efficiency is a core point of concern due to sharing of a single control channel among many participating stations with high mobility. Up to now, neighborhood aware content dissemination has only been considered for VANET security mechanisms, but not for other protocol layers. Thus, we show that extending on demand distribution of fixed or slowly changing data sets to all layers can reduce delay until full cooperative awareness about cooperating stations is achieved. Moreover, the developed strategy is able to reduce average bandwidth requirements. Thereby, the management entity foreseen in currently standardized VANET frameworks is used to coordinate content dissemination between different protocol layers. A simulation based evaluation is provided, which shows good performance of the proposed mechanism within the current ETSI ITS framework.**

I. Introduction

Vehicular ad hoc networks (VANETs) are about to enter the mass market in upcoming years. Thereby, similar approaches are used in Europe and USA within the ETSI Intelligent Transport Systems (ITS) and Wireless Access in Vehicular Environments (WAVE) frameworks, respectively [1], [2]. Both systems use a dedicated frequency band with low level access following the 802.11p standard.

Both VANET approaches use a single control channel with 10 MHz bandwidth to exchange safety critical information [3]. This kind of data is intended to be used for realization of future advanced driver assistance systems (ADAS) in order to enhance traffic safety. VANET messages are to be distributed by ITS-Stations (ITS-Ss), which can be distinguished into on board units (OBUs), to be typically found in mobile vehicles, and stationary road side units (RSUs).

The majority of data exchange in VANETs happens by cyclically distributed ITS-S's status messages. These are so called Cooperative Awareness Messages (CAMs) in ETSI ITS and Basic Safety Messages (BSMs) in WAVE. The majority of channel load occurring on the highly bandwidth limited control channel is caused by these messages. Thereby, it has been found that the achievable communication distance significantly suffers from increased channel load [4]. Thus, different mechanisms to limit channel utilization by individual VANET participants have been studied.

Channel usage by an ITS-S is mostly governed by rate of message generation. In WAVE the BSM generation rate is fixed to 10 Hz, while it varies from 1 to 10 Hz in ETSI ITS depending on a set of vehicle states, e.g., its speed. Moreover, the number of data sets (often called containers) contained in a message varies. On the facility layer dedicated optional containers are only included sporadically, but not in every single message [5]. Additionally, the message generation frequency can be limited by so called distributed congestion control (DCC) mechanisms. Furthermore, pseudonym certificate (PSC) distribution by the network layer security entity is controlled by a mix of cyclic and situation aware on-demand inclusion [6], [7]. Thereby, PSCs are piggybacked on higher level messages.

Unfortunately, limiting message generation or container inclusion rates limits the information quality for receivers (also called cooperative awareness quality [4]) as their update rate decreases. In prior work, all data sets have been treated equally in this regard. However, as recently found in [8], a large number of data sets within (almost) every message stay constant or change very slowly. Thus, such data sets do not need the update frequency provided by standardized message distribution mechanisms. Such mechanisms have been designed to fulfill required update rates for fast changing information, e.g., vehicle position. Moreover, facility layer data distribution does not regard the status of an ITS-S's neighborhood. Thus, significant delays can occur before required information is received at new communication partners after start of message exchange.

Hence, we provide methods to limit channel usage and reduce basic connection setup time without reducing quality of cooperative awareness. Firstly, a strategy to separate data sets according to their required update rates are studied. This is intended to suppress distribution of data already known to the surrounding to lower channel utilization. Secondly, a mechanism for cross layer on demand reaction to detected new neighbors is proposed. It is intended to reduce the time after initial message exchange between two ITS-Ss until they know about all of each others constant or slowly changing parameters, e.g., vehicle dimensions, which can be regarded as some kind of connection setup time. Lastly, we introduce a methodology to build more content aware metrics for VANET performance. In contrast to prior approaches, it takes the need of applications for data sets from different sources into regard.

The remainder of this work is outlined as follows. Firstly, a review of related work is given in Section II. Section III provides an analysis of configuration data exchange in VANETs based on ETSI ITS. Section IV introduces a cross layer approach to optimize configuration data dissemination. To evalu-

ate the introduced concepts, a method for content aware performance metrics is described in Section V. Section VI provides an evaluation about the achieved results. Finally, Section VII gives a conclusion together with possible topics of future work.

II. Related Work

At first, prior work in regard to typical characteristics of data exchange within currently suggested VANET approaches is reviewed. Secondly, metrics for assessing VANET performance are looked at.

A. Characteristics of Data Exchange Within VANETs

The biggest share of current VANET use cases focuses on applications using only broadcast information with no cooperative interaction between participants. Thereby, the majority of information exchange is done via cyclically sent status messages. Theses messages are called Cooperative Awareness Messages (CAMs) within ETSI ITS and Basic Safety Messages (BSMs) within WAVE. CAMs are distributed with varying frequency from 1 to 10 Hz depending on an ITS-S's dynamics, while BSMs are always sent with 10 Hz frequency.

So far, the only real interactive communication is done by the network layer level security entity, in order to distribute pseudonym certificates (PSCs) on demand. This happens by piggybacking PSCs on higher level messages depending on so called security profiles [6]. It has been shown that such on demand dissemination can significantly reduce channel load in many scenarios [9]–[11]. However, not including the PSC in every message can also lead to so called cryptographic packet loss, i.e., disregarded packets due to impossible verification. This leads to delayed awareness of other ITS-S's presence on higher communication layers (e.g., for facility layer services or applications). To minimize delays in PSC distribution, current standards use a combination of cyclic inclusion with implicit and explicit PSC requests. It has been shown that usage of such request schemes speeds up PSC exchange significantly [7].

On higher communication layers, e.g., facility level, the only introduced bandwidth saving mechanism is to vary the included parts of the overall data set in a cyclic manner. For example, the CAM facility (also called Cooperative Basic Service) only includes a low frequency container and all other optional containers (encapsulated in the special vehicle container) every 500 ms, while the highest CAM distribution frequency is 10 Hz [5]. So far no on demand distribution of data sets has been considered on layers above the network layer security. However, a CAM includes a significant number of data sets which do not or just slowly change over time [8]. Thus, cyclic distribution of this data sets will waste bandwidth in cases where all receivers already know about them. Hence, on demand distribution should be considered also on the facility layer to safe bandwidth on the single available control channel within ETSI ITS and WAVE.

Furthermore, no coordination of the information inclusion procedures on the different communication layers has been considered so far. Unfortunately, this can lead to a stacking up of multiple delay sources until the information is finally received by applications. This is pointed out in greater detail in Section III. In contrast to [12], delays on all layers are studied.

B. VANET Performance Metrics

Many different metrics have been introduced to measure the performance of a VANET. Simple metrics like channel busy ratio or packet delivery rate can only assess parts of VANET performance, but often improvement in regard to one metric makes another metric show worse performance. For example, inclusion of PSCs into every CAM removes cryptographic packet loss completely, but massively increases channel busy ratio [13]. Thus, metrics characterizing well trade offs between the different system parameters are required. Promising approaches are often referred to as cooperative awareness quality metrics [4].

However, none of these metrics has so far regarded variable content on the different protocol layers above the network layer security entity. Thus, these metrics assume that once a message has passed the receivers input verification, the receiver has full information about the sender. However, this is clearly not the case with many messages carrying only parts of the full information set of an ITS-S. Hence, we outline a possible way to overcome this weakness in Section V.

The common property of PSCs and (almost) constant data at other protocol layers is that they can be seen as some kind of configuration parameters. They need to be exchanged once after initial radio contact between ITS-Ss, in a procedure which is some kind of link setup being somehow in contrast to the fact that VANET communication is typically connection less. Afterwards, these parameters can be (re-)used often. To enable efficient handling of configuration data within ETSI ITS based VANETs, its characteristics are analyzed in the next section.

III. Configuration Parameter Exchange in ETSI ITS

The majority of information exchange in current ETSI ITS based VANETs is based on CAMs. Thereby, the included information sets on the facility and network layer are adjusted according to multiple system properties. This is done to keep channel load on the single control channel as low as possible.

The different information sets on the facility layer have been assigned to dedicated containers, e.g., the CAM basic container. These containers are always included at once. Currently, the CAM high frequency container is always included in CAMs alongside with the CAM basic container [5]. However, both containers include unchanging or hardly changing data sets, which are called volatile constant data in [8].

To reduce the size of CAMs, some configuration data is already assembled in the low frequency container. It is only distributed cyclically, but not within each CAM [5]. Thereby, the inclusion interval is fixed to 500 ms. However, constant data sets which are regarded as always required for applications still remain in the always included containers. In order to be able to move this data sets into the low frequency container, methods to minimize the initial reception delay at receivers are required.

Thereby, the following data sets from the CAM high frequency container and the CAM basic container could be moved to the low frequency container:

- station type (basic container)
- vehicle dimensions: vehicle length and width (high frequency container)
- curvature calculation mode (high frequency container)
- driving direction (high frequency container)

Furthermore, the individual data fields from the low frequency container should be optional and only set in case their values changed or distribution of all constant data to a newly detected neighbor is required. Thereby, special treatment is required for the path history field. Its values clearly change rapidly, however distribution is only required to inform new neighbors about the trajectory of the sending ITS-S. All other ITS-Ss can track the path of other ITS-Ss themselves from frequently received CAMs. Thus, there is no need to frequently distribute the quite long path history data set.

On the network layer level security entity a similar approach for bandwidth saving is already in use. Thereby, the PSC is not always included and can be replaced by its much shorter hash value [6]. A number of different mechanisms has been proposed to decide when to emit the full PSC, including work published in [4], [7], [9]–[11], [14]. Many of these works are (partly) based on a neighborhood discovery scheme, which has been shown to outperform pure cyclic information distribution [7], [10]. Such schemes have not been considered for the facility layer assembling of CAMs.

For all ITS-Ss having received the constant data from an ITS-S, repeated reception of this information can be regarded as overhead. The first reception of a CAM on the facility layer is bound to also receiving the PSC of the same ITS-S. Only in case the PSC is available to the security entity, the message can be verified. Otherwise, it is dropped and does never arrive at the facility layer. This means, to provide the constant data to a receiving ITS-S with minimal delay (which is no delay at all), the sender has to include all constant data in the message also carrying the PSC. Afterwards, transmission of both data sets, constant data and PSC, is superfluous, as no new information is provided to the receiver. Obviously, in case of a pseudonym change, both data sets have to be disseminated again.

Current day one ITS applications are based on just simple data dissemination by broadcasting of messages without real interaction between nodes in the VANET. However, future applications will be really cooperative. Thus, they will probably require to exchange some configuration data between cooperating entities. Such information is clearly to be exchanged once at the beginning of interaction and has only to be updated when is has changed. Furthermore, exchange of the required parameters should be fast, as node mobility is high in VANETs.

According to current standards, there is no coordination between the different protocol layers to synchronize the inclusion of specific data sets (often called containers on the ITS facility level). Therefore, the initial delay between the first message exchange on the network layer and the real usage of information in applications can stack up significantly over the separate protocol layers. This is because the exchange of configuration data can happen sequentially, while it could happen simultaneously with appropriate coordination between the different layers. The stacked up delay t_{total} can be calculated by

$$t_{total} = \sum_{n=1}^{N} t^n_{detect}.$$

Thereby, N is the number of lower level entities having to exchange data sets before the target functionality has access to all required data sets. For example, an application using the path history field from the CAM low frequency container has to wait for authentication causing t^1_{detect} (< 1s) and for emission of the particular container causing t^2_{detect} (< 0.5s), thus $N = 2$ holds. An illustration of this example is given in Figure 1.

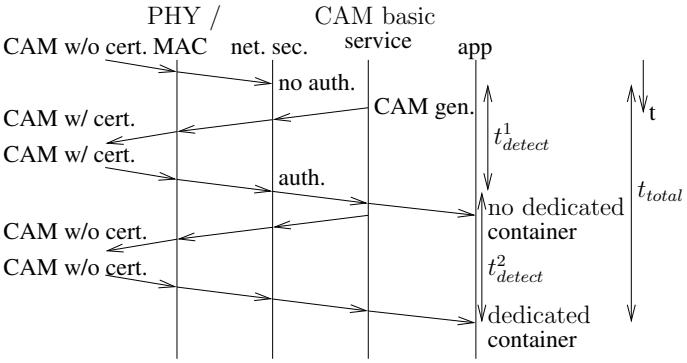

Fig. 1. Delay stacking up over multiple layers.

Clearly, applications requiring data from multiple sporadically distributed data sets can suffer from higher values of N and thus also t_{total}. Optimal cross layer coordination would yield $N = 1$.

A strategy for application of cross layer coordinated emission of configuration data within VANETs based on ETSI ITS or WAVE is discussed in the following Section IV.

IV. Cross Layer Aware Dissemination of Configuration Data

A generic concept for coordinated distribution of configuration data within VANET communication stacks is introduced in Section IV-A. Afterwards, misuse prevention is studied in Section IV-B and special advantages for rapid communication setup after pseudonym changes are described in Section IV-C.

A. General Concept

In order to realize an optimized data dissemination scheme considering all protocol layers the following criteria are taken into regard.

1) Channel load (i.e., channel busy ratio) should be as low as possible to minimize packet collisions and thus increase communication distance leading to higher cooperative awareness quality.
2) Delay from first radio contact between ITS-Ss to presence of required data sets at both of them should be minimized.

Clearly there is a trade off between delay and channel load, as always including all data sets would yield zero delay. However, cooperative awareness would greatly suffer from such

a dissemination strategy due to high channel load and thus short communication distances.

As outlined in Section III, there is clearly a requirement to coordinate the dissemination of configuration data between different ITS protocol layers. Thereby, the individual criteria of channel load as well as data dissemination delay can minimized and an optimized trade off between both can be achieved.

According to the standard ITS architecture the functionality coordinating different layers should be provided by the cross layer ITS management entity. Therefore, it should provide an interface for triggering the detection of a formerly unknown ITS-S. This interface should be used by the lowest level layer detecting new nodes in the ITS-S's neighborhood to inform all other layers about its finding. Moreover, the management entity should provide the possibility for arbitrary ITS-S functionality (e.g., the CAM basic service or any application) to subscribe for notifications in case the detection of a new ITS-S is triggered.

By coordinated emission of configuration data sets from all different layers the dissemination delay can be reduced to $t_{total} = t^1_{detect}$. This means, the delay caused by the lowest level layer cannot be avoided by the proposed strategy.

On the receiver side of an ITS-S, the network layer security entity is the first one to recognize the presence of a formerly unknown ITS-S in the surrounding of its own ITS-S. Thus, it should react with a trigger to the management entity, which can disseminate this information to further registered users of this information. There are two possibilities on when to do so, which are to do

1) insecure neighborhood detection (similar to standardized unsecured PSC requests [7]), which triggers detection after an unverifiable message from a formerly unknown node was received, e.g., a CAM without PSC, or to do
2) secured neighborhood detection, i.e., the detection is triggered after a new node was successfully authenticated.

Clearly, the biggest gain in delay avoidance can be expected from the first approach. Only in this case $N = 1$ can be achieved. Instead, the secured version can only reach $N = 2$. Moreover, unsecured dissemination of configuration parameters is already standardized for the security entity [6]. Reference [7] clearly shows the big gain in speeding up PSC exchanges by using this approach in comparison to its secured counterpart.

Furthermore, the above given approach will not lead to the usage of unauthenticated data sets within higher level applications. Received data will still only be handed over to them after it was properly authenticated.

B. Misuse Prevention

As outlined in reference [7], an attacker can use unsecured PSC requests to cause frequent inclusion of this data in other ITS-Ss' CAMs. In case of coordinated transmission of configuration data from multiple layers, the attacker could cause even higher data traffic and thus also channel busy ratio leading to the possibility of a denial of service (DOS) attack.

To overcome this possible design weakness, we propose to limit the inclusion rate of higher level configuration data. The limit of the maximum configuration data dissemination frequency $f_{prop,max}$ can be chosen to be equal to the currently standardized cyclic inclusion rate. Thereby, $f_{prop,max} = 2$ Hz would hold. Thus, the channel load increase in a system using cross layer coordinated distribution of configuration data would be equal to a system not using such coordination.

By the described methodology a DOS attack can be avoided, while normal (not attacked) systems can still profit from decreased delay and channel load due to cross layer coordination.

C. Configuration Data Distribution after Pseudonym Changes

An important use case for cross layer aware distribution of configuration parameters are pseudonym changes. Typically, connection setup in VANETs happens when ITS-Ss are quite far away from each other, i.e., when they get close enough to get into each others communication range. This is especially true for rural scenarios, e.g., on highways, with a low number of shadowing buildings and road crossings. However, this is not the case when an ITS-S changes its pseudonym.

According to current standards each ITS-S decides on its own when to change its pseudonym. Thus, from the perspective of surrounding ITS-Ss this happens at some random point in time. To avoid tracking, all protocol layers change their used IDs during the pseudonym change process. Therefore, other ITS-Ss have to regard the ITS-S as a new neighbor, which they know nothing about. Thus, all configuration data on all layers has to be exchanged anew. In this case the exchange process is especially time critical. ITS-Ss which need to exchange their parameters can be expected to be quite close to each other.

Even in case ITS-Ss cooperate during the pseudonym change process, this only means that an ITS-S can know when another ITS-S is about to change its pseudonym. However, it is an inherent property of pseudonym changing that no mapping of old ID to new ID of the same originator should be possible. Thus, all configuration data has to be exchanged anew.

V. Towards Content Aware Performance Metrics

Multiple different metrics for measuring VANET performance, e.g., cooperative awareness of an ITS-S, have been suggested, as outlined in Section II. However, none of these metrics takes different sources of required data sets, e.g., from within specific CAM containers or headers on different protocol layers, into regard.

Distinct applications typically use different data sets from VANET messages. These can be from dedicated CAM containers or even different message types. For example, an application may use data from CAM, TOPO (topology) and SPAT (signal phase and timing) messages to determine the optimal trajectory for passing a road crossing equipped with traffic lights.

Due to differing requirements, evaluation of individual applications requires dedicated parametrization of VANET performance metrics. Thus, a one fits all approach will hardly work for evaluation of different applications.

Hence, we propose to use metrics based on an analysis of data sets required by studied applications. Thereby, also intermediate layers supporting higher level protocols have to be considered.

Each used data field i has its own cooperative awareness metric $coop_i$. Moreover, it is assigned a weighting coefficient c_i and a presence indicator $p_i \in \{0; 1\}$. The value of p_i is zero in case i is not available at the ITS-S and one otherwise. For N used data fields, which contain $|M|$ mandatory data fields, overall cooperative awareness $coop$ is calculated by

$$coop = \left(\sum_{i=0}^{N} coop_i \cdot c_i \cdot p_i \right) \cdot \prod_{i \in M} p_i.$$

Thereby, M is the set of all mandatory data fields. In case all data fields are required $N = |M|$ holds. One can clearly see, that in case of a missing mandatory data field cooperative awareness is zero. This is motivated by the fact that pure knowledge that another ITS-S exists within communication distance does not enable any non-trivial application to work. Knowledge about the mandatory data sets of the detected ITS-S is required for this, e.g., its position.

The introduced weights c_i can be used to adjust the influence of the presence of dedicated data sets on the overall value of $coop$. Thereby, $\sum_{i=0}^{N} c_i = 1$ holds. In case all used data fields are mandatory, we suggest to assign equal weights to the individual data sets, i.e., $c_i = \frac{1}{N}$.

VI. Evaluation

Evaluation of the proposed cross layer coordination mechanism is split into two parts. At first, the used performance metrics as well as simulation environment are described. Secondly, achieved results are discussed in detail.

A. Performance Metrics and Simulation Environment

To assess VANET performance, we study the metrics of

1) delay until all data from a sporadically distributed CAM container (low vehicle container) is received as *coop* and
2) average message size of a CAM at the output of the network layer. This is used, as lower levels introduce a constant increase to message size, i.e., they do not use variable size data fields.

The delay is measured at the application level. Thereby, the application is assumed to require data from the high and low frequency container, but does not send any dedicated messages on its own. Moreover, exchange of PSCs is required to enable communication. Thus, $N = |M| = 3$ holds for $coop$. Equal weights are assigned to considered data fields.

The used simulation environment combines multiple dedicated tools. Thereby, the microscopic traffic flow simulator SUMO is used to generate realistic vehicle movement. Moreover, the network simulator ns-3 is used to simulate the wireless channel, physical and access layer of communication. Thereby, a two way ground model is used with urban scenario parameters as proposed in [15]. The remaining Car2X specific functionality is provided by the ezCar2X framework according to current ETSI ITS standards. For a detailed introduction of the simulation framework the reader is referred to [16].

The considered traffic scenario is a roundabout scenario, which is based on exporting a real road setup found in Munich Maxvorstadt from Open Street Map (OSM). Vehicle traffic is generated using the SUMO random trip generator. Additionally, the so called core zone concept is used. Thereby, the area in which the evaluation is performed is only a subset of the whole simulated area. This is done to avoid the influence of edge effects on the obtained results.

B. Results

According to [13] the size of a CAM without optional containers (like the low frequency container) is 42 bytes. Unfortunately, analysis of the influence of removing a data field from a CAM container is data dependent, due to the variable length encoding of the used ASN.1 UPER (unaligned packet encoding rules) scheme [17]. Thus, we use real data obtained from the ezCar2X implementation and a drive through Munich. Thereby, we find that the size of a CAM including the low frequency container with a full size path history field yields a CAM size of 389 bytes. Hence, including the the low frequency container can increase CAM size by more than a factor of nine. This clearly shows that one should try to avoid unnecessary inclusions of the contained configuration data.

Moreover, by moving the remaining configuration data from the high frequency container to the low frequency container we can realize high frequency CAM size of 38 bytes, while the size of a CAM including configuration data stays constant. Thus, high frequency CAMs can be shortened by about 9.5% in size on the facility layer.

Neglecting packet loss, extra delay at the facility layer after message acceptance by the security entity can be determined as follows. With 10 Hz CAM emission frequency, the chance of receiving the low frequency container at the facility layer without delay is just 20%. Thus, with 80% probability container reception is delayed between 100 and 400 ms. Hence, in average $\bar{t}^2_{detect} = 250$ ms holds.

With the cross layer neighborhood aware dissemination scheme from Section IV, the maximum delay is 100 ms, i.e., the interval between two successive messages. In this case, the average delay (on the facility layer) depends on the relation between the number of new pseudonym certificate receptions based on cyclic (i.e., cannot use cross layer coordination) and neighborhood aware (i.e., uses cross layer coordination) certificate emissions. In the case of a new certificate being received, because the sender emitted it due to cyclic emission, the delay will be 100 ms. Instead, in case of neighborhood aware emission, the delay will be zero, as the whole set of parameters required at all layers will be included.

The average delay for distribution of all configuration data after neighborhood discovery (i.e., recognizing a new node's presence) is illustrated in Figure 2. After the given time span $coop = 1$ holds, while before $coop = 0$ (in average) due to missing mandatory data from the low frequency container.

The increase of delay alongside with rising traffic density (i.e., lower vehicle interval) is caused by authentication delay, while the extra delay on the facility layer is constant. Moreover, the difference in delay between the coordinated and the uncoordinated emission scheme is quite constant with a value of about

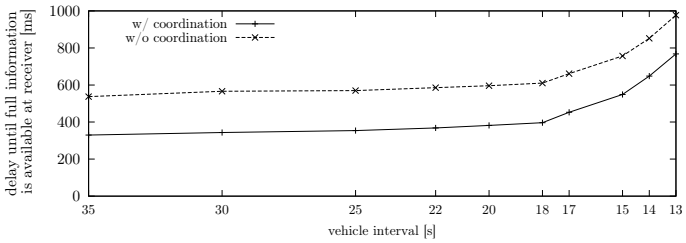

Fig. 2. Configuration data distribution delay under different traffic densities.

200 ms. Thus, the coordination mechanism clearly outperforms its standardized counterpart in regard to this metric.

The average number of inclusions of the low frequency container in CAMs within systems using or not using the cross layer approach from Section IV is given in Figure 3.

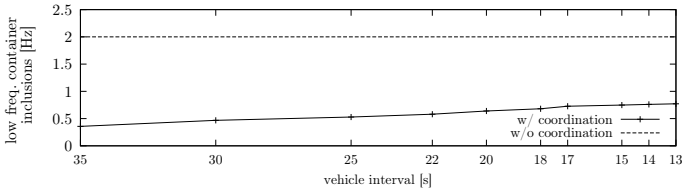

Fig. 3. CAM low freq. container inclusion rate for various traffic densities.

One can clearly see from the results provided in Figure 3 that, the proposed coordination scheme from Section IV outperforms is uncoordinated counterpart. Thereby, configuration data distribution rate is reduced by at least a factor of 2.5. As shown above, configuration data accumulates for the biggest part of CAMs if present. Thus, the amount of used bandwidth by each ITS-S is reduced substantially.

Confidence intervals for measured results were very small, so this information is not present in above given illustrations.

An overview about achieved results as well as possible topics of future work are given in the following section.

VII. Conclusion and Future Work

VANET technologies are about to enter the mass market during the next years. They require a rigid security system, due to used wireless communication. Moreover, intended usage for safety critical ADAS to increase traffic safety requires not only a secure communication, but should also provide low communication setup delays under strict bandwidth requirements.

Frequent dissemination of constant or slowly changing data sets adds overhead on different VANET protocol layers. Prior work has focused on pseudonym certificate distribution as a major source of overhead. However, we find that such kind of data is to be found on many protocol layers. We identify this data as configuration data, which only has to be distributed to each communication partner once and can be reused often. Furthermore, the initial distribution of the full set of configuration data over all layers is found to be a source of major delay during connection setup. We find that cross layer coordination can efficiently reduce this delay and even decrease transmission data rate at the same time.

Due to the shown benefits, we regard the proposed cross layer coordinated distribution of configuration data, as being well usage within future VANETs.

Future work can study the influence of the proposed cross layer coordination on dedicated applications. Moreover, the strategy can be extended for usage in hybrid communication scenarios using multiple technologies for dissemination of distinct data sets. Furthermore, the content aware performance metric scheme can be evaluated for more use cases.

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 et. al., "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); 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.

[4] 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.

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

[6] *Intelligent Transport Systems (ITS); Security; Security header and certificate formats*, ETSI Technical Specification 103 097, Rev. V1.1.1, Apr. 2013, v1.1.1.

[7] 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.

[8] S. Bittl and A. A. Gonzalez, "Privacy Issues and Pitfalls in VANET Standards," in *1st International Conference on Vehicular Intelligent Transport Systems*, May 2015, pp. 144 – 151.

[9] 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.

[10] 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.

[11] 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.

[12] A. Vinel, C. Campolo, J. Petit, and Y. Koucheryavy, "Trustworthy Broadcasting in IEEE 802.11 p/WAVE Vehicular Networks: Delay Analysis," *IEEE Communications Letters*, vol. 15, no. 9, pp. 1010–1012, July 2011.

[13] 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.

[14] 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.

[15] L. Cheng, B. E. Henty, D. D. Stancil, F. Bai, and P. Mudalige, "Mobile Vehicle-to-Vehicle Narrow-Band Channel Measurement and Characterization of the 5.9 GHz Dedicated Short Range Communication (DSRC) Frquency Band," *IEEE Journal on Selected Areas in Communications*, vol. 25, no. 8, pp. 1501–1516, 2007.

[16] 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.

[17] O. Dubuisson, *ASN.1 Communication Between Heterogeneous Systems*. OSS Nokalva, June 2000.