Mutual Influence of Certificate Distribution and Pseudonym Change Strategies in Vehicular ad-hoc Networks

Sebastian Bittl
HU Berlin
sebastian.bittl@mytum.de

Karsten Roscher
Fraunhofer ESK
karsten.roscher@esk.fraunhofer.de

Abstract

Vehicular ad-hoc networks (VANETs) are subject to high interest from both the automotive industry as well as government bodies due to their prospect of increasing safety of driving. Wireless data exchange within VANETs requires rigid security mechanisms to enable its usage in safety critical driver assistance systems. Requirements include not only authenticity and integrity of messages, but also privacy of drivers. We find that much research has been conducted on certificate dissemination and on privacy enhancing certificate (i.e., pseudonym) change. However, mutual influence of techniques from both domains has not been studied in prior work. Hence, we provide an analysis of such cross influence. We show that certificate change massively increases channel load under currently standardized certificate distribution mechanisms. Thus, we propose to use explicit signaling of certificate changes among nodes to limit the found overhead. The conducted evaluation shows that this approach overcomes the identified problems.

Index Terms

Pseudonym Change, Certificate Distribution, Channel Load, VANET, Privacy, Security;

I. Introduction

Vehicular ad-hoc networks (VANETs) are an active research area. Their intended use for increasing safety of driving leads to high interest of their mass roll-out in upcoming years, from both the automotive industry as well as government bodies. To realize this goal, data sets communicated in VANETs should enable future safety critical cooperative advanced driver assistance systems (ADAS).

To enable safety critical use cases, VANETs require a rigid security system. Otherwise, their wireless data exchange would expose them to straight forward attacks. Thus, public key cryptography is typically employed to sign messages [1]. Required meta data, e.g., public keys, for receivers is contained in certificates. VANETs are characterized by a high number of participants with high individual mobility. Hence, on demand exchange of certificates between communicating nodes is required, as pre-distribution of all certificates to all nodes in the VANET is infeasible. Additionally, privacy of drivers is endangered by vehicle tracking in VANETs. Such tracking is straight forward, in case each vehicle distributes a unique data set, like node identifiers on various protocol layers or the node's certificate. Hence, each node changes its certificate together with all node identifiers on all protocol layers frequently to protect its privacy by avoiding node tracking.

Prior work in the ad-hoc network domain has either focused on certificate distribution or certificate change, which is part of a pseudonym change, strategies. However, cross influence of strategies from both domains has not been studied in detail. A complex certificate distribution strategy has been developed within European Telecommunication Standards Institute (ETSI) Intelligent Transport Systems (ITS) and Wireless Access in Vehicular Environments (WAVE) frameworks being major approaches towards realization of VANETs in practice. In contrast, none of these standardized frameworks holds any details about certificate change strategies [2]. However, regulatory bodies and users clearly demand privacy conserving usage of VANET technologies, especially in Europe [3], [4].

We provide a detailed analysis of the mutual influence of standardized certificate distribution strategies and commonly suggested certificate change algorithms. We find that certificate change has a major negative impact on the channel load by leading to superficial certificate distribution. This is caused by the neighborhood aware certificate distribution strategy, which is part of currently standardized certificate distribution mechanisms. Explicit signaling of a performed certificate change is recommended as a countermeasure. The conducted evaluation shows that this approach works well.

The further outline is as follows. Related work is looked at in Section II. An analysis of the mutual influence of common certificate distribution and certificate change algorithms is provided in Section III. Moreover, a countermeasure to the found VANET performance decrease is suggested, which requires only minor overhead in messages. An evaluation of the proposed approach is given in Section IV. Finally, Section V provides a conclusion about achieved results

together with possible topics of future work.

II. Related Work

Communication within a VANET serves two important classes of use cases. These are safety critical and non-safety critical, e.g., entertainment, use cases. Many non-safety critical use cases make use of IP-based communication. In contrast, dedicated communication protocols are have been developed for safety critical use cases, i.e., usage of VANET based communication as a data source for cooperative advanced driver assistance systems. This work concentrates on safety critical communication in VANETs. Hence, the reader is referred to [5]–[7] for topics regarding non-safety critical use cases of VANETs.

The main data exchange in VANETs happens via cyclically broadcast beacon messages, which are called Cooperative Awareness Messages (CAMs) in ETSI ITS and Basic Safety Messages (BSMs) in WAVE. Both systems use a maximum sending frequency of 10 Hz. However, ETSI ITS adapts this distribution frequency to vehicle's dynamics and experienced channel load between 1 and 10 Hz, while WAVE always uses 10 Hz [5], [8].

VANET-based communication faces the challenges of high node mobility, a large range of possible node densities and limited communication range of each participant. An additional challenge is given by the choice of using only a single communication channel for safety critical message exchange in major VANET approaches ETSI ITS in Europe and WAVE in the USA. Hence, available bandwidth for message exchange is highly limited [5]. Therefore, mechanisms to keep message length and message sending frequency, both influencing the channel load, to an acceptable limit are required [5], [9], [10].

The given characteristics of the communication system lead to the development of protocol stacks, which are mostly stateless, i.e., most messages are usable on their own and there is almost no connection setup procedure [5]–[7]. This also holds for the security systems of ETSI ITS and WAVE, which are outlined in the following.

An overview of the security system used by current VANET approaches can be found in [1]. Typically, a public key infrastructure (PKI) based on a multi-level certificate hierarchy is used. A common set of root certificates is assumed to be known to all nodes. All other types of certificates, i.e., the ones of certificate authorities (CAs) and individual nodes in the network, are distributed on demand. In doing so, piggybacking of certificates on regular messages is used [11], [12].

To secure individual messages, these are signed using (typically) asymmetric key cryptography, and the digital signature is appended to the message. The signature is part of a so called security envelope, which is handled at the network layer. The security envelope is also used to distribute all meta data, which is required to verity the message at each receiver, e.g., the sender's certificate. In case a receiver cannot verify a message due to an unknown sender's certificate, the message is dropped leading to so called cryptographic packet loss. Sporadic inclusion of certificates into the security envelope is used to limit channel load by shorting of messages. Different strategies on when to include a node's certificate have been developed [13]–[16].

For privacy protection, nodes use each single certificate only for a limited time. Otherwise, this data set could be used as a unique identifier for each node. Thus, trivial node tracking could be performed by an attacker. This behavior leads to the often used term pseudonym certificate (or simply pseudonym) for the individual certificates of nodes. Many different certificate change schemes have been suggested, e.g., mix zones, silent periods, and combinations of the individual mechanisms [2], [17]. No message sending takes place within a silent period. Mix zones are an extension of the silent period concept with spatial concentration of certificate changes to well defined areas. Placement of mix zones is studied in [18].

The most straight forward approach to perform a certificate change is uncoordinated certificate change. Each vehicle decides on its own when to change its pseudonym, e.g., periodically after a fixed time span. This approach is popular, because it does not inflict communication overhead for coordinating vehicles to perform the change, works under all traffic densities and does not need pre-configuration of dedicated mix zones [2], [3].

Moreover, different kinds of cooperative pseudonym change strategies have been developed, in which the place of a pseudonym change is negotiated between participants in an ad-hoc manner. However, such strategies typically suffer from bad performance in case of sparse traffic density [2]. Pseudonym change signaling in cooperative approaches happens before the change is performed by each node. Required information is piggybacked on regular beacon messages. No signaling of a conducted pseudonym change after the change happened, as used in this work, has been considered so far.

The impact of certificate change strategies on application performance is studied in [19]. However, the impact on certificate distribution is not looked at. Change of used certificates has been identified as an extra source of certificate distribution in VANETs in [20]. Each certificate change leads to the appearance of a "new" node and all other nodes include their certificate

in the next beacon message, due to neighborhood aware certificate emission. However, no detailed analysis of this influence has been provided yet. The importance of the neighborhood aware certificate emission mechanism within the complex certificate distribution strategy used by current ETSI ITS (and WAVE) standards has been shown in [15]. Thus, simple discarding of neighborhood aware certificate emission is not an appropriate countermeasure to the found extra source of overhead. Hence, a study on mutual influence of certificate distribution and change strategies is provided in Section III.

III. Cross Influence of Certificate Handling Aspects

In general mutual influence between certificate distribution and change algorithms can occur in both directions assuming an ETSI ITS or WAVE conforming protocol stack. A

1) certificate change always
    a) creates the need to distribute the new certificate of the node which changed its certificate, and
    b) triggers the detection of a new neighbor at other nodes, which receive the new certificate. According to the standardized certificate distribution algorithms, this causes every receiver to include its own certificate into its very next beacon message [11], [12]. However, the distribution of all these unchanged certificates has to be considered unnecessary overhead, as these certificates are already known by its expected receivers. Thus, certificate changes may undermine the bandwidth saving approaches of well known certificate distribution strategies, which try to limit the inclusion rate of certificates into beacon messages.
2) Certificate distribution can cause the detection of an address duplication. [21] suggests to change the used certificate in case the lower 32 bits of a node's own certificate ID are identical to the ones of a received certificate's ID. Other kinds of duplicate address detection mechanisms are discussed in [22]. The certificate change then again causes influence no. 1.

One should note that alternative certificate distribution strategies not using neighborhood aware certificate emission are not affected by case no. 1b [14]. However, such strategies have not been considered for usage in ETSI ITS or WAVE. Hence, they are not considered in the following, as we focus on VANETs resembling current standards.

The probability of case no. 2 is quite small, while case no. 1 happens regularly during standard operation of a VANET. Moreover, case no. 2 always causes case no. 1. Thus, our focus is on case no. 1 in the following.

A. General Analysis

In the following analysis we assume the certificate distribution strategy from current VANET frameworks ETSI ITS and WAVE [11], [12], [15]. This includes a combination of cyclic, neighborhood aware (or implicit request) and explicit request based mechanisms. For an in-detail study of the influence of individual sub-mechanisms the reader is referred to [15].

1) Uncoordinated Certificate Change: In case no coordination of certificate changes among nodes takes place, an equal distribution of such changes over time can be assumed. A node always changes its certificate after a fixed time span, as suggested in [3], [19], [23]. Thus, there will be steady presence of certificate changes going on in the VANET. The amount of such changes experienced by a single node depends on the amount of other nodes within its communication range and the certificate change interval.

We denote the number of certificate changes experienced by a single node within its one-hop vicinity per time interval between two successive beacons by c_i. Assuming a fixed beacon frequency f (in WAVE 10 Hz), for all nodes,

$$c_i = \frac{n_{i,known}}{\bar{t} \cdot f}$$

holds. $\bar{t}$ denotes the average time interval between certificate changes in seconds. There is no use in changing certificates faster than sending messages. Hence, $t \geq \frac{1}{f}$ holds. This also means that $\max c_i = n_{i,known}$, i.e., the number of certificate changes experienced during interval i between two beacon emissions can at most be equal to the number of known nodes within the nodes environment $n_{i,known}$.

n gives the number of nodes within communication range of a node (i.e., within its one-hop neighborhood), with N being the set of all such nodes ($|N| = n$). N consists of two disjoint sets, the set of known nodes N_{known}, i.e., such from whom at least one message has been received before, and the set of unknown nodes $N_{unknown}$, i.e., such from whom no message was received before. The relation between these sets can be expressed by the following equations.

$$N_{known} \cup N_{unknown} = N; N_{known} \cap N_{unknown} = \emptyset,$$

$$n_{i,known} = |N_{i,known}|, n_{i,unknown} = |N_{i,unknown}|,$$

$$n = n_{i,known} + n_{i,unknown}.$$

In practice, c is not a fixed value, but changes frequently, as both the communication range of a node as well as its surrounding traffic density vary. Moreover, within ETSI ITS f can vary between 1 Hz and 10 Hz.

Figure 1 gives an illustration of values for c_i, which can be expected in practice. A range of nodes within communication range from 1 to 400 nodes is assumed [1]. Certificate change intervals t with 10 s, 30 s and 5 minutes (= 300 s) are taken from recommendations in [3], [24], [25]. The maximum number of certificate emissions per second is given by the maximum number of CAMs sent per second. This is due to the piggybacking strategy, which is used for certificate distribution, i.e., the need to distribute a certificate cannot trigger sending of a message on its own. A maximum CAM emission frequency of $f = 10Hz$ is used within ETSI ITS [8]. Hence, the maximum number of certificate inclusions per second is ten. This is illustrated by the *always include limit* in Figure 1.

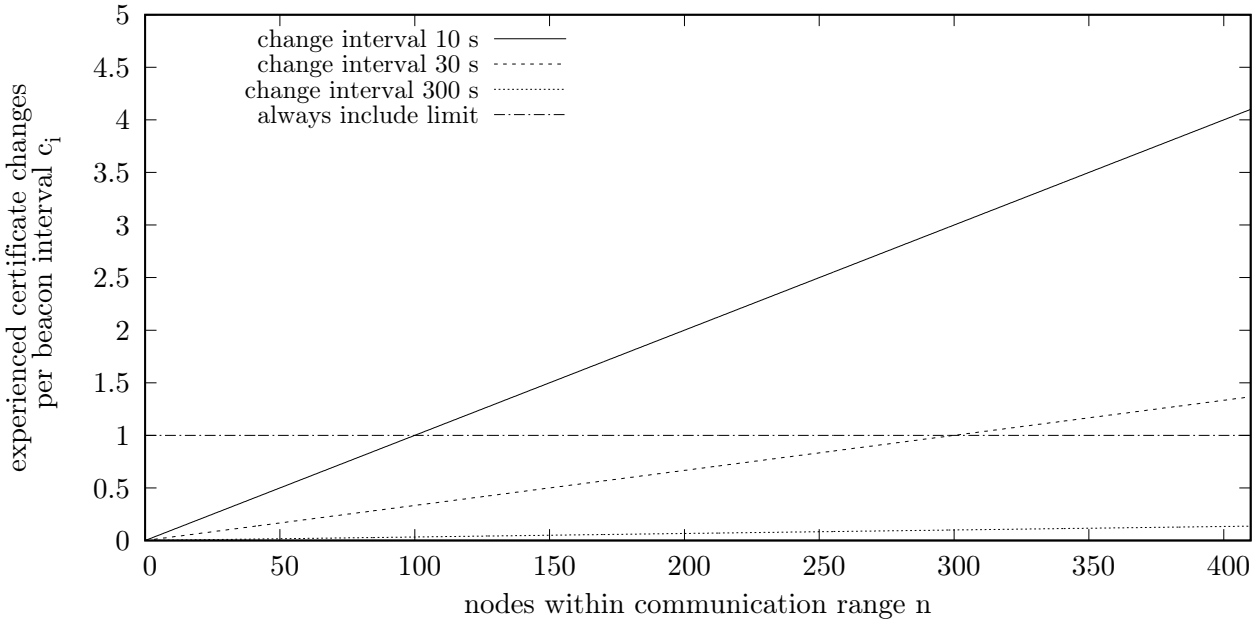

Fig. 1. Number of new nodes detected only due to pseudonym changes between two successive beacon emissions ($f = 10$ Hz).

Provided values in Figure 1 show that c_i significantly increases with shorter certificate change intervals. Thus, the impact of certificate change on neighborhood aware certificate distribution is lower for higher values of t. However, high values of t result in lower levels of node privacy [24], [25].

Results in Figure 1 show that for high node densities, $c_i \geq 1$ holds, i.e., between the emission of every CAM and the next CAM a new neighbor gets detected. Hence, neighborhood aware certificate distribution leads to inclusion of the full certificate in (almost) every emitted beacon message. Multiple newly detected neighbors within the time interval between sending of two beacons do not further increase the emission frequency in comparison to a single new neighbor (saturation effect). Thus, a certificate inclusion frequency close to f can be expected.

Results from prior work show that much smaller certificate inclusion frequencies have to be used to achieve required high cooperative awareness levels among nodes, i.e., well awareness of nodes about their surrounding [2], [13], [14]. This holds especially for high density traffic scenarios. Too high certificate inclusion frequencies lead to increased channel load increasing the probability of collisions on the wireless channel. Thus, the available communication area is reduced, which limits availability of information for applications [2], [14]. Hence, such behavior should clearly be avoided.

The outlined VANET behavior is independent from whether a silent period is used after the certificate change or not. However, one should note that the length of the period during which awareness about the affected node by other nodes is poor is longer than the silent period itself. After the silent period, the certificate of the node has to distributed as well to restore awareness.

2) Mix Zone based Certificate Change: Following the mix zone concept certificate changes are performed within well defined geographical areas realizing some coordination between nodes. The minimum size of a mix zone depends on the tolerated tracking probability by an attacker even if a node changed its certificate within the mix zone. Larger mix zones reduce the success rate of an attacker [2].

Algorithms for the placement of mix zones have so far only considered privacy aspects. However, pseudonym change can significantly limit the abilities of applications as shown in [19]. To keep such negative impact as small as possible, the areas affected by pseudonym changes should be kept as small as possible. A sketch of a mix zone together with the affected area is given in Figure 2.

One can see from Figure 2 that the affected area is bigger than the mix zone itself. The core reason for this behavior is that once nodes leave the mix zone, they have to start to distribute their individual data sets, e.g., their certificate, anew. Every node leaving the mix zone is recognized as a new neighbor by all other nodes. Due to neighborhood aware certificate distribution, the area close to the border of the mix zone will steadily experience increased channel load. Thus,

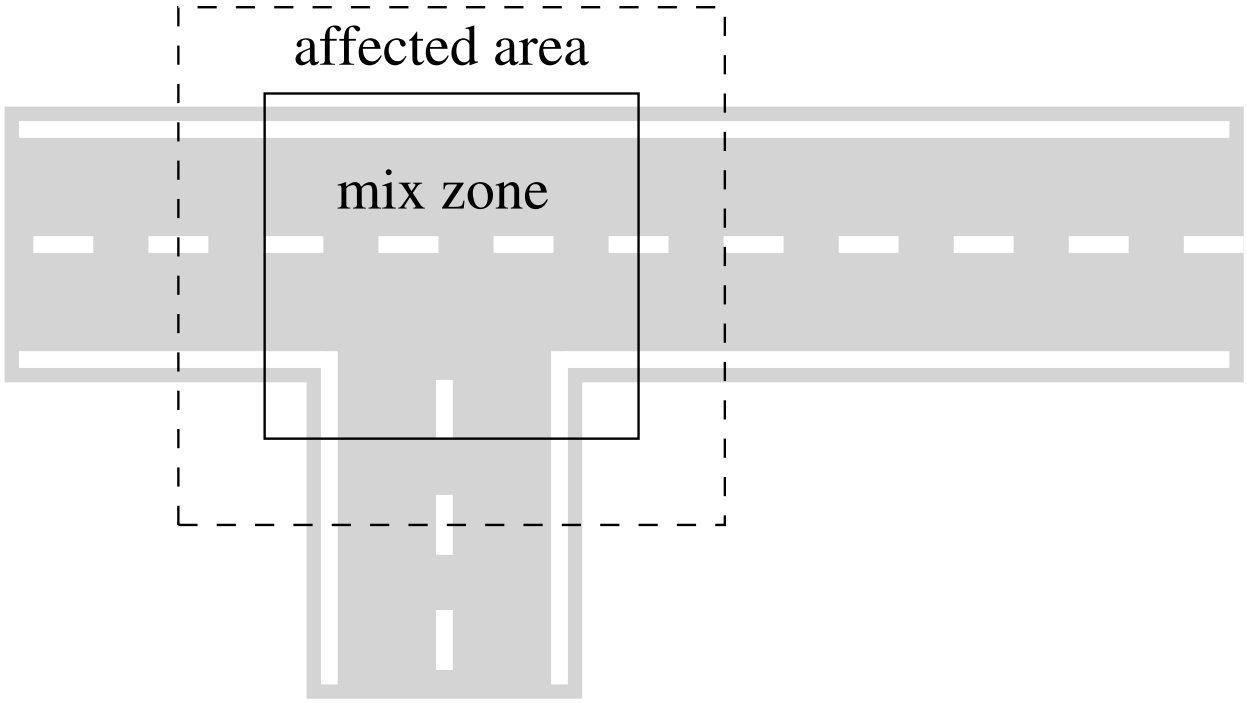

Fig. 2. Sketch of a mix zone and the area affected by the pseudonym changes.

nodes inside that area will suffer from higher packet loss ratios and lowered communication radius.

The amount of channel load increase around the mix zone depends on the traffic flow emerging from the mix zone into its surrounding. More vehicles per time interval leaving the mix zone will increase the new neighbor detection rate, which leads to more frequent certificate exchange causing increased overhead. The size of the area around a mix zone, which is influenced by the additional certificate exchanges, only depends on the wireless channels characteristics (assuming channel load independent sending power and beaconing rate).

In comparison to the case of uncoordinated certificate change, the VANET is only affected in parts from the presence of the cross influence of certificate distribution and change strategies. However, the size of areas with unreliable VANET performance is increased. Thus, methods to limit the influence of negative impact from certificate change on VANET performance are discussed in Section III-B.

3) Cooperative Certificate Change: During a cooperative certificate change procedure, participants, which are geographically close to each other, change their certificate simultaneously. The location of the change is found in an ad-hoc manner, in contrast to fixed mix zones. Moreover,

not all nodes in vicinity have to take part. Different approaches on how to select cooperation partners have been proposed [2].

As for other certificate change techniques, evaluation has so far focused on the level of privacy obtained from the cooperative strategies. However, from an application's perspective it is also important to consider the time until cooperative awareness has recovered after a pseudonym change. This recovery time relates to a geographical area around the ad-hoc found pseudonym change area. The size of this extra area of low cooperative awareness clearly depends on communication conditions after message sending starts again at participating nodes.

In case of poor communication conditions, e.g., high channel load, recovery time and thus, the area of poor cooperative awareness will increase. Hence, the superficial certificate emissions caused by the coordinated certificate changes have a negative effect on VANET performance, like in the case of mix zones discussed above.

For cooperative certificate change strategies, the locations of changes are not fixed. Thus, the performance impact of certificate change is spread over the whole VANET. This can even increase the need for low recovery times, as the performance impact can not be limited to well defined areas, i.e., well placed fixed mix zones. In case all nodes within a dedicated area take part in the certificate change process, the performance impact is equal to the one of a mix zone being present in that particular area, i.e., nodes set up an ad-hoc mix zone.

B. Countermeasures to Negative Impact

As outlined above, the core reason of the channel load increase by certificate change is the neighborhood aware certificate emission strategy. However, removing this mechanism from the certificate distribution process leads to a significant decrease in overall cooperative awareness of nodes [15].

Another possibility to avoid the found problem is to introduce a mechanism, which enables a node changing its certificate to tell others about this change after the change was performed. This can be done by introduction of a new optionally included header field in the security envelope. Moreover, no detailed data has to be present in this field. Thus, it needs no payload, but pure presence of the field can show that this message is not to be treated as an implicit certificate request. Hence, the size of this field can be limited to one byte, which is just its identifier [11], [12]. The field is only present in the first beacon to be sent after a certificate change, to minimize impact of this strategy on overall VANET performance.

One could argue that the presence of an indicator for a recent certificate change adds to the information available to an attacker. However, the amount of leaked information should be very small due to the following reasons. When an attacker observes a node with a new pseudonym there are just two possibilities on how this could happen. Either a node changed its pseudonym or a new node was just started up. The new introduced certificate change indicator resolves that ambiguity. However, the attacker already has many options to resolve the ambiguity by considering the different data sets in the message. For example, a node with a velocity significantly different from zero will not be a ”really new” one, as nodes start transmitting immediately after their start up. Moreover, the node's position can be used in conjunction with map data, as nodes do not appear at certain places like in the middle of a motorway or similar places. Thus, we consider the additional information exposed to the attacker as negligible.

An extra positive aspect of the pseudonym change indicator is that nodes with identifiers no longer in use can be actively removed from caches within receivers, e.g., a local dynamic map (LDM) as used in ETSI ITS [26]. This avoids to have multiple cached instances of a single real node, which are not known to be identical in the real world, due to conducted pseudonym changes. So far, only timeout based approaches have been suggested to limit such issues in VANETs [26]. To tolerate message loss, used timeout values are selected to be longer than message sending intervals. Hence, after a pseudonym change a node is known to its surrounding by (two) different pseudonym identities. This may confuse ADAS, which need to know positions of nodes within the neighborhood. Thus, reliability of communicated data sets as a data source for cooperative ADAS can be increased by using a certificate change indicator.

IV. Evaluation

We apply simulation based evaluation for the concepts discussed in Section III. The simulation environment is discussed in Section IV-A. Achieved results are given in Section IV-B.

A. Simulation Environment

The simulation environment of the ezCar2X framework is used to evaluate the concepts described above. The framework implements an ETSI ITS conforming protocol stack. Details of its implementation can be found in [27]. For simulation purposes the protocol stack from ezCar2X is used together with the ns-3 network simulator [27], [28]. In doing so, ns-3 is used to model the physical layer and parts of the access layer, while the remaining protocol stack is

provided by ezCar2X. The channel model uses pathloss and Nakagami fading, as implemented within ns-3, with parameters taken from [29].

The used traffic scenario features deterministic traffic flow on a freeway generated by the microscopic traffic flow simulator Simulation for Urban Mobility (SUMO) [30]. The freeway has three lanes in each direction and is 6 km long. Presented results are assembled within the core zone of the simulation (4 km long), which is surrounded by additionally simulated area to avoid edge effects. The scenario is illustrated in Figure 3. All nodes receive a random internal start-up time to avoid unrealistic synchronization of the time based beacon emissions.

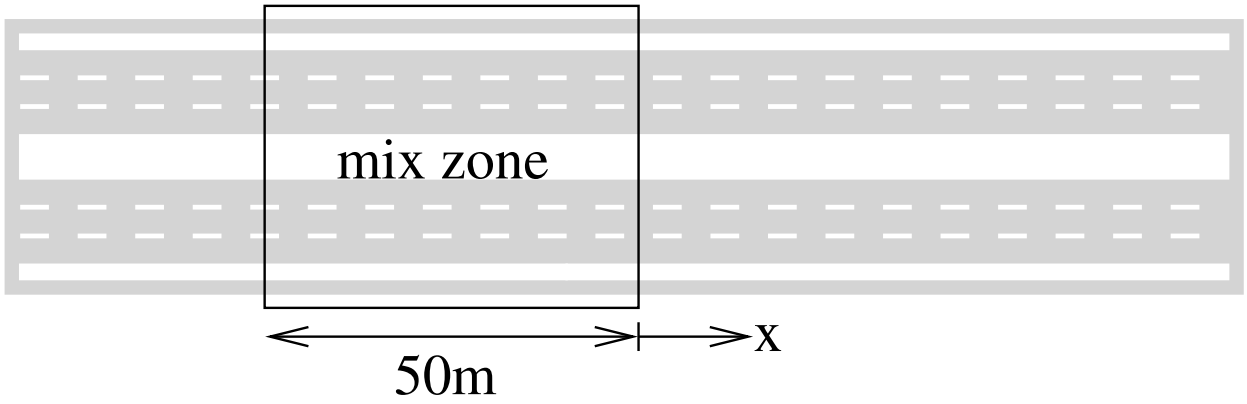

Fig. 3. Freeway scenario used for evaluation.

Our metric to measure the impact of certificate change strategies on the standardized certificate distribution mechanism is the channel busy ratio (CBR). It has been shown that average communication range and cooperative awareness of nodes suffer significantly from an increase in CBR. Thus, low CBR values are required to enable robust and reliable applications [5].

The uncoordinated and time based pseudonym change strategy uses a pseudonym timeout of 30 s. For the mix zone concept, the rectangular shaped mix zone is 50 m long (sides in parallel to the road boundaries) and spans all lanes, as shown in Figure 3. No beacon emission takes place within the mix zone. All vehicles know about the mix zones presence in advance, i.e., its presence is pre-configured. This scenario also resembles an on-demand cooperative pseudonym change in which all nodes within the mix zone participate. The realization of cooperative pseudonym change follows the proposal in [31].

B. Results

Within the used traffic scenarios, the experienced average maximum communication distance of vehicles is about 300 m. The obtained results for the uncoordinated certificate change mechanism from current standards are given in Table I. The average node interval on the road characterizes the traffic density. Thereby, an interval of 2 s is used to cause high traffic density, while an interval of 9 s leads to quite low traffic density. Moreover, the standard deviations of obtained results for the CBRs are given in the last column of Table I.

scenario (node interval)	average CBR in %	σ^2
without signaling (2 s)	55.0	1.67
with signaling (2 s)	40.5	1.79
without change (2 s)	39.5	1.52
without signaling (9 s)	22.2	1.61
with signaling (9 s)	15.9	1.73
without change (9 s)	15.7	1.71

TABLE I

CHANNEL BUSY RATIOS FOR UNCOORDINATED CERTIFICATE CHANGE WITH AND WITHOUT EXPLICIT SIGNALING OF THE CHANGE.

The CBR experienced in the reference scenario without ongoing pseudonym changes (*without change*) gives a lower bound for the results of scenarios with pseudonym changes. Results from Table I show that the constant level of CBR is massively increased by using uncoordinated pseudonym change in the standardized form, i.e., without pseudonym change signaling (scenarios *without signaling*), in comparison to the reference scheme. In contrast, the scenarios with such signaling (*with signaling*) show much lower CBR levels. Moreover, comparison with the reference scenario without any pseudonym changes happening shows that there is only a minor increase in the average CBR by the approach using signaling. Furthermore, the difference of obtained averages is smaller than the standard deviations. Hence, the difference can be regarded as being only of minor significance.

The increase in CBR by ongoing pseudonym changes is found to be higher for a higher traffic density, i.e., a lower node interval, in Table I. This can be expected, as a higher traffic density relates to more nodes experiencing the pseudonym change. Hence, more nodes detect a new neighbor in the scenario without signaling, which causes them to superficially include their pseudonym certificate in the next message.

Results from Table I also show that the CBR increase by ongoing pseudonym changes cannot be completely overcome by the proposed signaling approach. This has two reasons. At first, this is do to additional pseudonym certificate emissions done by nodes changing their pseudonym. These extra certificate emissions are required and cannot be avoided. Secondly, message loss on the wireless channel causes some nodes within the neighborhood of a node changing its pseudonym to not receive the first message after the change, which also holds the pseudonym change signaling flag. Hence, these nodes do not profit from the conducted pseudonym change signaling and behave like in the scenario without such signaling. However, simulation results showed that the number of affected nodes is always low in the considered scenario (< 1 %).

The results on channel load around a mix zone are displayed in Figure 4. The given distance is the one from the border of the mix zone, as nodes do not emit beacons within the mix zone. For each traffic density the scenario with (*with sig.*) and without explicit pseudonym change signaling (*w/o sig.*) is provided.

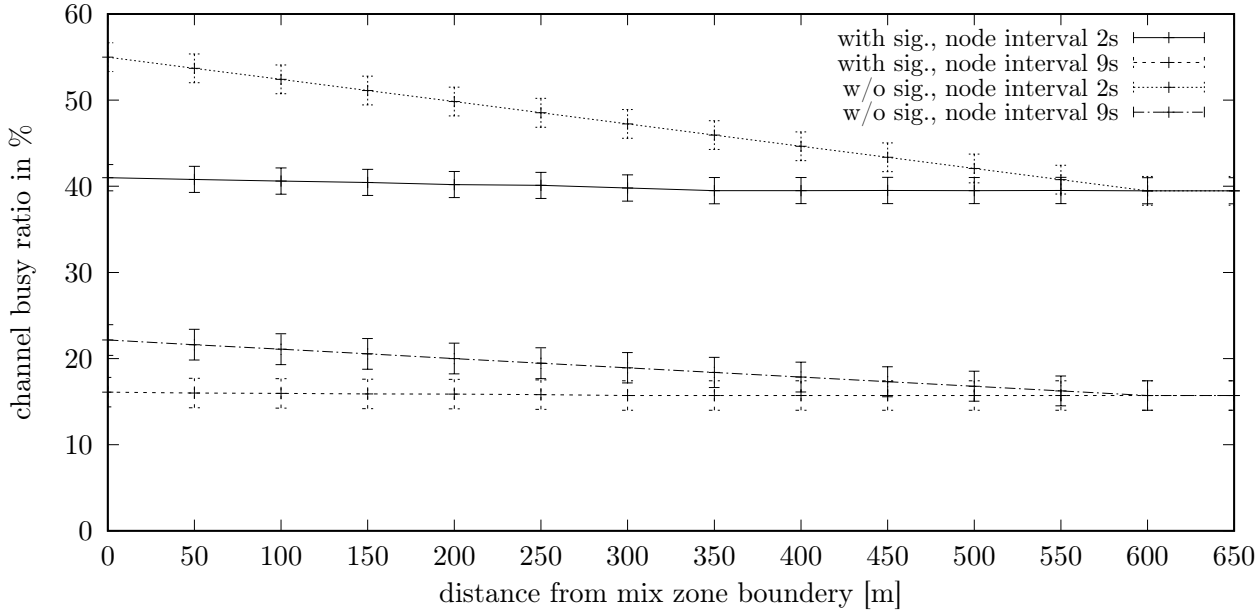

Fig. 4. Channel load around a mix zone.

One can see from Figure 4 that the CBR drops to the level without the mix zone's presence at about two times the average communication distance (about 600 m). The given errors bars illustrate the standard deviation of obtained measurement results. As these are quite small, one can regard the shown results as reliable. Results for the reference scenario are not displayed to

avoid overloading the figure. They are very close to the ones for the approach using signaling, as found for the scenario of uncoordinated pseudonym changes.

Moreover, in the area close to the mix zone the CBR is significantly increased without signaling of certificate changes. In contrast, CBR is only marginally increased in average around the mix zone, when explicit signaling of the pseudonym change is used. This increase is mainly caused by the nodes leaving the mix zone and immediately emitting their new pseudonym certificate. Moreover, a minority of other nodes does not receive the new certificate during its first emission due to packet loss. Thus, they detect a new node when receiving further beacons from the nodes leaving the mix zone. However, the given results show that there is only a very small impact of this behavior on the CBR.

Results for the implemented coordinated certificate change scheme are very similar to the ones given above for fixed mix zones. No measurable impact of the coordination overhead on the overall channel load could be found. Hence, the discussion given above for fixed mix zones also applies for the considered coordinated certificate change strategy.

The provided results show that the introduction of a pseudonym change indicator in the security envelope is a simple, but yet effective countermeasure to negative influence of pseudonym change on VANET performance, which is caused by unintended influence of pseudonym change on neighborhood aware certificate distribution. Hence, we recommend the proposed approach for inclusion into future ETSI ITS and WAVE standards.

V. Conclusions and Future Work

VANETs are an important approach towards increased safety of driving. To realize the required security system a PKI approach with on demand certificate exchange and privacy conserving certificate change has been developed. However, these two major topics have only been treated separately in prior work. We show that significant mutual influence between both topics exists.

Uncoordinated certificate change is shown to almost disable the bandwidth saving influence of sporadic certificate inclusion in messages. This leads to high channel load, especially in high density traffic scenarios. Moreover, popular certificate change concepts of MixZones and cooperative pseudonym change are also shown to significantly increase channel load decreasing overall VANET performance. Hence, straight forward combination of certificate distribution and certificate change algorithms is discouraged. Instead, a dedicated mechanism enabling efficient combinations of algorithms from both domains is required.

We propose to introduce a dedicated certificate change indicator and show that it can almost completely overcome the found performance decrease. Thus, its inclusion should be considered in future VANET standards.

Future work can study the influence of combined certificate distribution and change strategies on further bandwidth saving strategies. These include distributed congestion control (DCC) [9] or further on demand data set exchange [10].

REFERENCES

[1] T. Schütze, "Automotive Security: Cryptography for Car2X Communication," in *Embedded World Conference*, Mar. 2011, pp. 1–16.

[2] J. Petit, F. Schaub, M. Feiri, and F. Kargl, "Pseudonym Schemes in Vehicular Networks: A Survey," *IEEE Communication Surveys & Tutorials*, vol. 17, no. 1, pp. 228 – 255, Mar. 2015.

[3] 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.

[4] Schmidt, J. and Eckert, K. and Schaaf, G. et. al., "Nutzerakzeptanz, IT-Sicherheit, Datenschutz und Schutz der Privatsphäre," Sichere Intelligente Mobilität Testfeld Deutschland simTD, Tech. Rep., Jun. 2013.

[5] C. Campolo, A. Molinaro, and R. Scopigno, Eds., *Vehicular ad hoc Networks - Standards, Solutions, and Research*. Springer, Dec. 2015.

[6] L. Delgrossi and T. Zhang, *Vehicle Safety Communications: Protocols, Security, and Privacy*. Wiley, Nov. 2012.

[7] C. Sommer and F. Dressler, *Vehiclular Networking*. Cambridge University Press, 2015.

[8] *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. V1.3.2, Nov. 2014.

[9] M. S. Bouassida and M. Shawky, "A Cooperative and Fully-distributed Congestion Control Approach within VANETs," in *9th International Conference on Intelligent Transport Systems Telecommunications*, Oct. 2009, pp. 526–531.

[10] S. Bittl, "Efficient Distribution of Static or Slowly Changing Configuration Parameters in VANETs," in *9th International Workshop Nets4Cars*, Oct. 2015, pp. 301 – 306.

[11] *Intelligent Transport Systems (ITS); Security; Security header and certificate formats*, ETSI Technical Specification 103 097, Rev. V1.2.1, June 2015.

[12] *IEEE 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. 2013, Apr. 2013.

[13] 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.

[14] 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.

[15] 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, M. Kassab et al., Ed., vol. 9066. Springer, May 2015, pp. 72–83.

[16] ——, "Efficient Rate-Adaptive Certificate Distribution in VANETs," in *Twelfth International Symposium on Wireless Communication Systems*. SCITEPRESS Digital Library, Aug. 2015, pp. 371 – 375.

[17] L. Huang, K. Matruura, H. Yamane, and K. Sezaki, "Enhancing Wireless Location Privacy using Silent Period," in *IEEE Wireless Communications and Networking Conference*, 2005, pp. 1187–1192.

[18] Y. Sun, B. Zhang, B. Zhao, X. Su, and J. Su, "Mix-zones Optimal Deployment for Protecting Location Privacy in VANET," *Peer-to-Peer Networking and Applications*, vol. 8, no. 6, pp. 1108–1121, 2015.

[19] S. Lefévre, J. Petit, R. Bajcsy, C. Laugier, and F. Kargl, "Impact of V2X Privacy Strategies on Intersection Collision Avoidance Systems," in *IEEE Vehicular Networking Conference*, Dec. 2013, pp. 71 – 78.

[20] S. Bittl, K. Roscher, and A. A. Gonzalez, "Security Overhead and its Impact in VANETs," in *8th IFIP Wireless Mobile Networking Conference*, Oct. 2015, pp. 192 – 199.

[21] Buburuzan, T. et al., "Draft C2C-CC Standards System Profile," CAR 2 CAR Communication Consortium, Tech. Rep., Jan. 2014, v1.0.4.

[22] S. Bittl, "Distributed Cross Layer Duplicate Address Handling for Safety Critical VANET Communication," *Vehicular Communications*, vol. 6C, pp. 1–6, Oct. 2016.

[23] *Intelligent Transport Systems (ITS); Security; Stage 3 mapping for IEEE 1609.2*, ETSI Technical Specification 102 867, Rev. V1.1.1, June 2012.

[24] E. Schoch, F. Kargl, T. Leinmüller, S. Schlott, and P. Papadimitratos, *Security and Privacy in Ad-Hoc and Sensor Networks, Third European Workshop, ESAS 2006, Revised Selected Papers*. Springer, 2006, vol. 4357, ch. Impact of Pseudonym Changes on Geographic Routing in VANETs, pp. 43–57.

[25] B. Wiedersheim, Z. Ma, F. Kargl, and P. Papadimitratos, "Privacy in Inter-Vehicular Networks: Why simple pseudonym change is not enough," in *Seventh International Conference on Wireless On-demand Network Systems and Services*, Feb. 2010, pp. 176–183.

[26] *Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Local Dynamic Map (LDM)*, ETSI European Norm 302 895, Rev. V1.1.1, Sept. 2014.

[27] 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*. vwh, Oct. 2014, pp. 51 – 62.

[28] 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.

[29] L. Cheng, B. E. Henty, F. Bai, and D. D. Stancil, "Highway and Rural Propagation Channel Modeling for Vehicle-to-Vehicle Communications at 5.9 GHz," in *IEEE Antennas and Propagation Society International Symposium*, Jul. 2008, pp. 1–4.

[30] 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.

[31] D. Eckhoff, C. Sommer, T. Gansen, R. German, and F. Dressler, "Strong and Affordable Location Privacy in VANETs: Identity Diffusion Using Time-Slots and Swapping," in *IEEE Vehicular Networking Conference*, Dec. 2010, pp. 174–181.