Effective Certificate Distribution in ETSI ITS VANETs Using Implicit and Explicit Requests

Sebastian Bittl, Berke Aydinli, and Karsten Roscher

Fraunhofer ESK, 80686 Munich, Germany
{sebastian.bittl,berke.aydinli,karsten.roscher}@esk.fraunhofer.de

Abstract. Security and privacy of current Car-to-X systems heavily depends on the usage of pseudonym certificates. These carry the required information for authenticating messages received from other vehicles. However, only a limited amount of detailed studies about certificate distribution strategies in VANETs as well as attack surfaces of such systems has been proposed. Therefore, a general study about possible distribution mechanisms and their parametrization is provided in this work. Thereby, the management of entries in request lists is identified as a key issue for system performance. Additionally, a design flaw in the currently standardized ETSI ITS distribution scheme is outlined leading to the possibility of an attacker significantly increasing channel load on the safety critical control channel. A solution to this problem is suggested and an evaluation of its performance is provided. Furthermore, the evaluation shows the great influence of request list management on authentication delay and thus on security inducted packet loss.

Keywords: Certificate distribution, VANET, ETSI ITS, security.

1 Introduction

Wireless Car-to-X communication systems, often called vehicular ad hoc networks (VANETs) like ETSI intelligent transport systems (ITS) in Europe [1], are in the wake of deployment in upcoming years. Thereby, security and privacy issues of such systems are a core point of concern. The main reason for this is the intended use for safety critical applications, even during so called Day 1 use cases from 2015 on. Thus, a security scheme for VANET messages has been developed and is in the still ongoing process of standardization [4,17].

Privacy of VANET users is commonly protected by a pseudonym scheme using changing pseudonym certificates to authenticate messages, e.g., Cooperative Awareness Messages (CAMs). Thereby, tracking of vehicles can be avoided or at least hindered [11]. However, usage of such authentication schemes in VANETs requires to distribute pseudonym certificates frequently alongside with data used by applications. Without the corresponding certificate received messages cannot be verified and thus are not provided to higher level applications [4].

Recent work in the area of certificate distribution in VANETs can be found in [9,10,12,13,16]. Moreover, current ETSI ITS and WAVE standards specify a

M. Kassab et al. (Eds.): Nets4Cars/Nets4Trains/Nets4Aircraft 2015, LNCS 9066, pp. 72–83, 2015.
DOI: 10.1007/978-3-319-17765-6_7

system using a combination of different mechanisms proposed in literature [2,4]. However, prior work has not studied the influence of different sub-mechanisms specified in ETSI ITS and WAVE on overall certificate distribution performance. Moreover, the design of the used explicit certificate request scheme has not been standardized in detail. Thus, we provide a proposal for how to manage explicit requests and show its suitability as well as significant influence on system performance during our simulation based evaluation.

The remaining part of this work is outlined as follows. Section 2 gives an overview about current state of the art regarding certificate distribution in VANETs and open issues in this area. Moreover, we point out a newly discovered security flaw in the mechanism of implicit certificate requests. Afterwards, Section 3 describes proposed enhancements to prior distribution strategies. Section 4 introduces the simulation environment used for further evaluation alongside with the studied traffic scenarios. Furthermore, the obtained evaluation results are discussed. Finally, Section 5 provides a conclusion about the achieved results.

2 Certificate Distribution in VANETs

Basically, VANET pseudonym certificates (PSCs) are distributed by embedding them into the so called security envelope of a message. In both ETSI ITS and WAVE, the security envelope is constructed at the network layer. This means that certificates can only be distributed when high layer functionalities, e.g., the CAM facility, trigger sending of a new message [2,4].

Instead of including the full PSC an ITS-station (ITS-S) can choose to just include an eight byte hash value (obtained via SHA-256) of the certificate. This is done in order to make the overall message shorter to save bandwidth on the wireless channel. The impact of this mechanism is quite significant, as the size of the security envelope is reduced to about 50% of its size compared to the case of a full certificate being included [7].

There are mainly three different kinds of certificate distribution techniques in ETSI ITS and WAVE based VANETs [2,4]. These are

1. always include the certificate,
2. cyclic certificate emission and
3. request based certificate distribution.

In regard to ETSI ITS, the first strategy is used for Decentralized Environment Notification Messages (DENMs) and all messages secured with the *generic* security profile [4]. The reason for this is the assumption that information distributed via DENMs is highly time critical. Thus, no so called authentication delay can be accepted for the corresponding use cases. An authentication delay occurs when a message is received from another ITS-S whose certificate is unknown because it is neither appended to the current message nor had it been received before.

For CAMs (or BSMs in WAVE) the second as well as third pseudonym certificate distribution strategy is used [2,4]. In both standards the cyclic PSC inclusion frequency is fixed. Additionally, a certificate request scheme, with some concepts similar to the proposals from [16], is used.

A congestion based PSC emission approach is proposed in [9,10]. However, comparison in these works is done only with the individual strategies given above, but not with the combined strategy used in current standards. Furthermore, no details on the request scheme in the systems used for comparison of the new approach is given in [9,10]. Thus, congestion based PSC distribution is not considered in this work, as it focuses on the influence of different certificate request mechanisms within the ETSI ITS framework.

For further analysis we separate the discussion of the certificate request scheme from standards [2,4] into the two cases of implicit and explicit requests.

2.1 Implicit Certificate Request

According to [4] each sent CAM serves as an implicit PSC request to any other ITS-S who has not received the current PSC of the sender. This means, that after receiving a message from a formerly unknown ITS-S the receiver includes its own certificate in the very next CAM. This concept is described as neighborhood aware certificate omission in [16].

The reason behind this rule is the assumption of a symmetric communication relation, i.e., a new ITS-S who just appeared in communication range is assumed to not know about the receiver as the receiver did not know about the sender. However, while this technique of certificate distribution has the potential of reducing authentication delay, it also causes a significant security issue.

The issue arises from the fact that any received CAM from a newly discovered ITS-S triggers inclusion of the full certificate in the next CAM of every receiver. This means that the sender does not need to authenticate itself to the receiver to cause the inclusion. Thus, a malicious user (attacker) can frequently send out CAMs without included certificate using a changing random hash value as his identifier and thereby cause every receiver to send its certificate in its next CAM. Thereby, the attacker causes the receivers to include the full certificate in (almost) every CAM. This will lead to increased channel utilization (in about two times the communication range of the attacker) and thus the communication conditions become more difficult for legitimate users. An attacker can try to use this mechanism to perform a denial-of-service (DOS) like attack on a VANET.

In order to analyze the DOS weakness we separate the implicit request scheme into two parts. These are

1. unsecured implicit certificate request and
2. secured implicit certificate request.

An unsecured request occurs in case a station receives a message (e.g. CAM) from another ITS-S whose PSC it does not know and the message only includes the digest of the other ITS-S's PSC. This means that the digital signature of the received message cannot be verified. Given the fact that maximum CAM emission frequency is 10 Hz and regular certificate inclusion happens with 1 Hz [4,5] in ETSI ITS (or 2 Hz in WAVE), one can assume that the majority of messages is broadcast without including a full PSC.

This means that unsecured implicit PSC requests are more likely to happen than secured ones. Therefore, the influence on system performance of skipping this kind of requests in order to avoid the above described DOS weakness can be expected to be significant.

A secured implicit certificate request occurs in case an ITS-S receives a message from a formerly unknown station which included the station's full PSC. Thus, the message can be verified using its digital signature.

An evaluation of the influence of (not) using the different kinds of implicit requests on overall system performance is provided in Section 4.

2.2 Explicit Certificate Request

An explicit PSC request can be performed by including a shorted version of the SHA-256 hash value of the PSC into the so called *request unrecognized certificates* header field of the security envelope. This header field includes a list of up to six entries [4]. However, the standard [4] does not specify how to manage these entries at all. Obviously, a request should not be repeated if it was successfully answered, however multiple different possibilities exist in other cases. Thereby, two main aspects can be differentiated.

First of all, it is considered how to handle new requests when there are more pending (i.e., not sent) requests than available places in the request list. Significant options are to

- drop new entries when the list is full,
- buffer new entries, but do not throw away already present entries or to
- maintain the list in a FIFO (first in first out) manner in which a new entry replaces the oldest one.

The second aspect to be studied is how to treat an entry after it was sent. Possibilities include mainly to

1. only include a request once (remove after sending) or to
2. repeat the request. Multiple possibilities exist for this strategy including
   (a) repeating for a fixed time (remove by timeout),
   (b) repeating for a fixed number of requests or
   (c) a combination of both.

It would also be possible to repeat a request until it is answered. However this is probably not a good strategy in VANETs due to the high mobility of participants. This can easily lead to a situation in which only a single packet can be exchanged between two ITS-Ss. In this case, the repeated requests just lead to unnecessary overhead.

Choices 2a and 2b differ in general due to the adaptive CAM emission frequency varying in the range from 1 Hz to 10 Hz (see [5] for CAM generation rules). This means that fixing the number of requests can only roughly control the time span for which a request is repeated. Assuming that the connectivity between vehicles is mainly time dependent (due to node mobility), we select 2a for our evaluation given in Section 4.

2.3 Attack on Certificate Distribution

As outlined in Section 2.1, the unsecured implicit certificate request mechanism leads to the possibility of an attacker being able to cause regular ITS-S to unnecessarily send their full certificate. Thereby, the channel load is increased and communication conditions become more difficult. In case the VANET has enough spare bandwidth the attack potential can probably be tolerated, but in case of an already highly used communication channel countermeasures are required.

A straight forward way to avoid the described weakness would be to not respond to unsecured implicit certificate requests. However, this could even make the overall situation worse. The reason being that the entire system of explicit certificate requests depends on using information from unverified messages. In case of the described attack it will flood the request lists of ITS-S with bogus entries and thereby it becomes highly unlikely that correct requests are sent out.

Given a system without support for unsecured implicit requests, the effect of the attack on used channel bandwidth will probably be small, as only three bytes are used for a single explicit certificate request [4]. However, the performance of the whole explicit request scheme can be expected to decrease significantly due to the lack of correctly sent requests. In such a situation the PSC distribution solely depends on cyclic certificate inclusion and secured implicit requests.

Section 4.5 provides an evaluation of the attacks influence on overall system performance as well as the efficiency of the outlined countermeasure.

3 Proposed Certificate Distribution Strategy

Based on the analysis of available PSC distribution strategies from Section 2, a new strategy is proposed in the following. It is based on the combination of methods from [4], but specifies the different strategies in greater detail.

Firstly, we keep cyclic PSC distribution with 1 Hz as in [4]. Moreover, all kinds of implicit PSC requests (secured and unsecured) are used. These are the quickest ones of all PSC distribution strategies, as they do not require any kind of interaction between stations. Additionally, they do not cause any extra overhead, like sending of extra data fields as used for explicit PSC requests.

Furthermore, our approach uses an explicit PSC request scheme with repeated requests. Thereby, we maintain the request list in a FIFO manner. This is motivated by the high mobility of ITS-S in VANETs. Thereby, stations tend to leave the communication range of the ego vehicle quite fast. This means that ITS-S whose CAMs were received lately are more likely to receive a response than those whose CAMs had been received earlier. Moreover, entries are dropped from the list after not receiving any message from an ITS-S whose PSC was requested for more than one second (remove by timeout). The one second time span was chosen to be equal to the maximum time span between sending of two CAMs by an ITS-S. As the CAM generation rate varies, entries are not removed from the request list after a fixed number of requests (see also Section 2.2).

A simulation based evaluation of the suggested certificate distribution strategy is given in the following Section 4.

4 Evaluation

In order to evaluate the performance of the distribution strategy proposed in Section 3 a simulation based approach is used. Thereby, the influence of the different sub-mechanisms of the combined approach is also studied. Furthermore, the influence potential of the DOS attack described in Section 2.1 on systems using implicit PSC requests is studied. Therefore, the used simulation environment, studied scenarios and achieved results are described in the following.

4.1 Simulation Environment

To evaluate PSC distribution strategies a simulation environment utilizing multiple tools is used. Thereby, the well known traffic flow simulator SUMO [6] provides realistic vehicle mobility. Furthermore, the wireless connections between vehicles are modeled with the network simulator ns-3 [14] with an integrated full ETSI ITS compatible C2X protocol stack. This stack is provided by the ezCar2X framework. The wireless channel modeling follows the results from [8]. A detailed description of the simulation framework can be found in [15].

4.2 Scenarios

To evaluate the above described PSC distribution mechanisms two different road network scenarios are used. In both full penetration of C2X technology in all vehicles is assumed.

The first scenario is a variant of the well known freeway scenario. Thereby, a deterministic traffic flow is assumed on all six lanes (three in each direction). The vehicles' intervals and speeds on different lanes are adjusted as given in [3].

For the second scenario, the road network was build up by exporting a representation of the real world roundabout found in Munich Maxvorstadt from Open Street Map (OSM). The resulting network was imported into SUMO and traffic flows were generated using the SUMO random trip generator. The simulation was run multiple times with different values for the initial random seed to achieve statistically significant results.

Both scenarios use the concept of a so called core zone [3,13] to avoid edge effects. Thereby, statistics are only collected inside a geographical subset of the whole simulation scenario, which is surrounded by an additionally simulated area.

4.3 System Performance Metrics

In our evaluation we use three different metrics to describe the performance of certificate distribution in VANETs. These are,

- average authentication delay,
- average number of discarded messages of ITS-S in close vicinity of the ego vehicle whose PSCs are unknown and
- average receive data rate as a metric for the channel load.

Thereby, the authentication delay is determined as the time difference between reception of the first message from an ITS-S and the reception of the ITS-S's certificate. The minimum of this time span is zero, in case the first received message contains the full certificate.

The second metric is inspired by prior work in [10]. It is assumed that it is more important to know the certificates of vehicle in close vicinity of the ego vehicle than it is to know the ones of more far away ITS-S. We chose a cyclic area with radius 200m as the core area of interest around each ITS-S. This metric is called cryptographic packet loss in [10].

4.4 Simulation Results Without Attacker

For both used road topologies the following certificate distribution schemes are taken into regard during the evaluation:

1. ETSI ITS based scheme from Section 3 using repeated explicit requests,
2. strategy 1 without repeated explicit certificate requests (onetime requests),
3. strategy 1 without unsecured implicit requests,
4. strategy 2 without unsecured implicit requests,
5. strategy 1 without any implicit requests,
6. strategy 2 without any implicit requests,
7. strategy 3 without any explicit requests (i.e., only secured implicit requests),
8. the always include strategy as a reference scheme.

In the following, we use the above given numbering scheme to refer to the individual strategies.

Strategy 7 is the only one which does not require to use any information from messages whose digital signature cannot be checked due to an unavailable full certificate. As the attack outlined in Section 2.3 makes the unsecured information used for explicit request almost unusable, this strategy resembles worst case system performance in case of an active attack (see also Section 4.5 below).

Firstly, results for the average authentication delay for the freeway scenario are given in Fig. 1. The x-axis is given in reverse order, as it displays the average time between two successive vehicles (as e.g., used in [13]). With decreasing time intervals between vehicles the traffic density increases.

One can see from Fig. 1 that strategy 1 clearly outperforms its alternatives. The authentication delay is much smaller, which means certificates are exchanged significantly faster. It is only outperformed by the always include strategy, which features no authentication delay at all. However, this strategy leads to excessive channel usage as illustrated in Fig. 5 and Fig. 6 later on.

Furthermore, one can clearly see the major impact of the certificate request strategy on system performance. All strategies using repeated requests clearly outperform their respective counterparts using just one-time requests.

Fig. 2 gives the authentication delay results for the roundabout scenario. As for the freeway scenario, strategy 1 outperforms its alternatives. Due to lower vehicle mobility and a smaller geographical setup absolute numbers are lower for the roundabout scenario (Fig. 2) compared to the freeway scenario (Fig. 1).

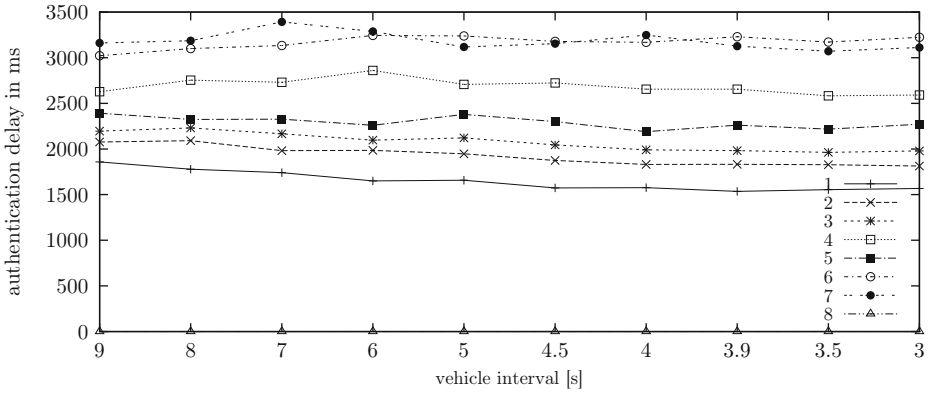

Fig. 1. Authentication delay in a freeway scenario with varying traffic density

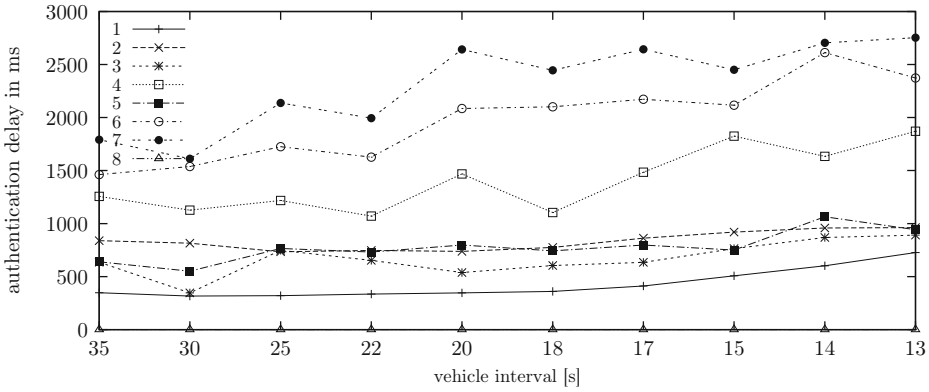

Fig. 2. Authentication delay in a roundabout scenario with varying traffic density

The results described above for PSC distribution strategies are clearly supported by the metric of the number of discarded messages from vehicles with unknown PSCs in a car's vicinity as illustrated in Fig. 3 and Fig. 4. Again strategy 1 clearly outperforms its alternatives except of reference scenario 8.

One can clearly see a negative impact on system performance by disabling the unsecured implicit certificate request mechanism (strategy 3) from Fig. 1, 2, 3 and 4. The authentication delay as well as the cryptographic packet loss increase significantly compared to strategy 1. This holds for strategy 2 vs. strategy 4, too. Fully disabling implicit requests further decreases system performance as exhibited by results for strategies 5 (vs. 3) and 6 (vs. 4).

From all provided simulation results, one can clearly see that strategy 7 provides a bad system performance, which is thereby shown to highly depend on using unverified information. Thus, disabling this mechanisms to guard the system from attacks is probably not a good solution in practice.

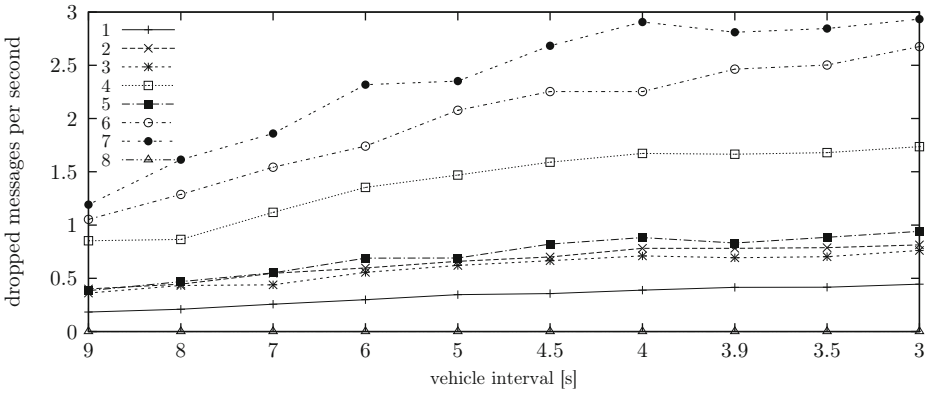

Fig. 3. Number of received messages from vehicles with unknown PSCs (cryptographic packet loss) in 200 m vicinity in the freeway scenario

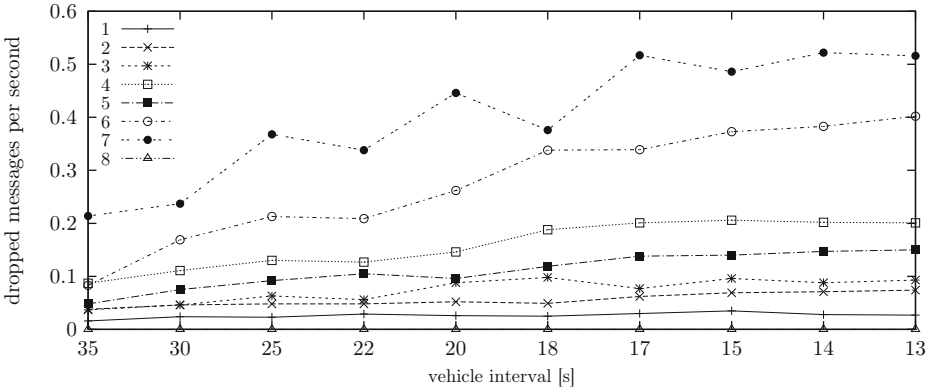

Fig. 4. Number of received messages from vehicles with unknown PSCs (cryptographic packet loss) in 200 m vicinity in the roundabout scenario

Figure 5 shows the average receive data rate of vehicles in the freeway scenario. One can see that the for all distribution strategies, except of the always include one (strategy 8), the results for this metric are very similar. Thus, strategy 1 also performs well in regard to the criterion of caused channel usage.

Figure 6 illustrates the obtained results for the receive data rate of vehicles in the roundabout scenario. The overall data rates are lower in this scenario compared to the ones in the freeway scenario due to significantly lower traffic density. However, the general trend of numbers as well as the relation between results for the different certificate distribution strategies is the same for the roundabout scenario as it is for the freeway scenario.

Moreover, our simulations also show that the additional requests for certificates generated by the optimistic approach do not lead to a significant increase

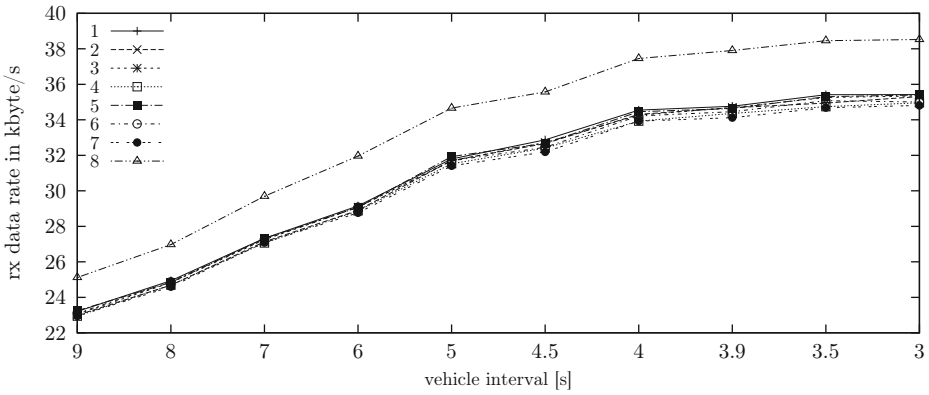

Fig. 5. Receive data rate in a freeway scenario with varying traffic density

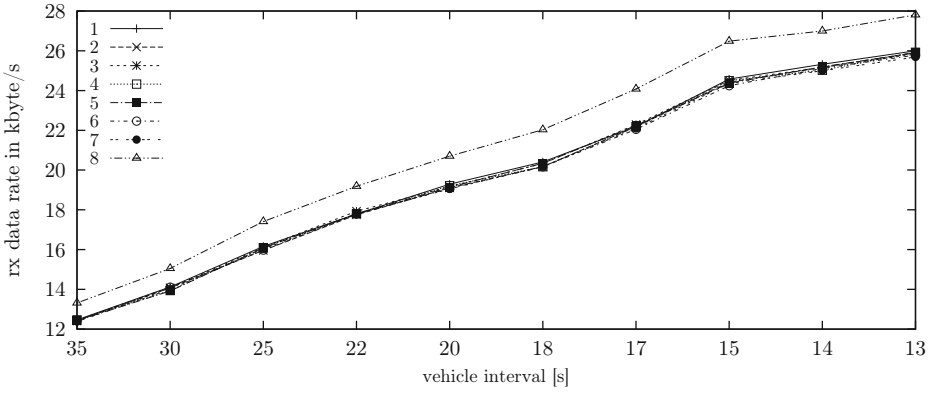

Fig. 6. Receive data rate in a roundabout scenario with varying traffic density

of the channel load. For all tested scenarios the increase was smaller then 1‰. Thus, one can conclude that using the optimistic approach can significantly increase certificate distribution performance of VANETs.

4.5 Simulation Results with Attacker

Two alternatives are considered for handling the DOS attack from Section 2. Either one accepts increased channel load and leaves its handling to other mechanisms like distributed congestion control (DCC) or one disables unsecured implicit requests. We use a single static attacker who sends out CAMs from an RSU with new identifiers at 10 Hz frequency (upper bound from regulators).

For both considered scenarios our results show that the attack cannot congest the wireless channel with certificate distribution strategy 1 (see Section 3) in use. Thus, the attack causes increased channel load but is not able to prevent ITS-S from regular communication. Thus, the attacked system works as the always

send strategy in regard to metrics of authentication delay and cryptographic packet loss. Therefore, the corresponding graphs are not given here again and the reader is referred to preceding Section 4.4 instead (see Fig. 1, 3, 2 and 4).

Although the attack renders the explicit certificate request mechanism unusable, we do not see any negative effect of this aspect when using strategy 1. The reason for this is the availability of enough spare channel capacity to send all messages with embedded full certificate via the manipulated unsecured implicit request scheme. Thus, explicit requests are never required and the failure of that mechanism does not cause decreased system performance in our scenarios.

The increase in receive data rate within communication range r of the RSU is significant for both considered scenarios. It even slightly exceeds the channel load generated by the reference strategy 8 sending the certificate in every message. This is caused by explicit certificate requests. The request list of attacked ITS-S is always full, while in the reference strategy 8 there is no request list at all. Outside r the channel load decreases and reaches the normal value at about $2 \cdot r$.

Disabling unsecured implicit requests as a countermeasure to the attack (see Section 2.3), does not lead to acceptable results for studied scenarios. Authentication delay and cryptographic packet loss show significant performance degradation, which almost reaches the upper bound given by strategy 7. However, an increase in channel load (caused by regular ITS-S) can be avoided as expected. As the attack cannot exhaust the system's spare channel capacity in the given scenarios, we do not recommend to disable unsecured implicit certificate requests. This may change in future scenarios with higher regular channel utilization leading to a decrease in available spare channel capacity.

In both scenarios our evaluation of the DOS attack clearly shows the impact of the attack. Within the RSUs communication range the channel load increases significantly. However, the system has enough spare communication capacity to avoid serious consequences of the attack. Advanced mechanisms, like attack detection and selective disabling of certificate distribution mechanisms, to conquer the outlined attack are out of scope of this paper and are subject to future work.

5 Conclusion and Future Work

Securing Car-to-X communication between ITS-S in VANETs is gaining importance in the wake of mass deployment of such systems. Thereby, an acceptable trade off between fast security mechanisms and their overhead in regard to communication bandwidth has to be achieved.

The attack potential of a static single attacker on currently standardized certificate dissemination was shown. Thereby, it was found that even in quite densely populated scenarios the attack is not able to congest the wireless channel so far that a successful DOS attack would be possible. However, for future extensions of communication in VANETs the attack has to be considered as it requires the system to have a significant spare bandwidth available to avoid harmful impact of the attack on overall system performance.

Furthermore, the major influence of the explicit certificate request strategy on overall system performance is shown. A novel strategy for managing request

lists is proposed and evaluated against different alternatives. Thereby, the proposed system clearly outperforms its alternatives. Thus, the proposed certificate request strategy should be regarded for usage in future VANET systems like ETSI ITS and WAVE.

Future work can study advanced mechanisms to limit the impact on used channel bandwidth caused by the outlined DOS attack on currently standardized pseudonym certificate distribution strategies.

References

1. Memorandum of Understanding for OEMs within the CAR 2 CAR Communication Consortium on Deployment Strategy for cooperative ITS in Europe (June 2011)
2. Draft Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages, P1609.2, D12 (January 2012)
3. Intelligent Transport Systems (ITS); STDMA recommended parameters and settings for cooperative ITS; Access Layer Part (2012)
4. Intelligent Transport Systems (ITS); Security; Security header and certificate formats (2013)
5. Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service (August 2013)
6. Behrisch, M., Bieker, L., Erdmann, J., Krajzewicz, D.: SUMO - Simulation of Urban MObility: An Overview. In: SIMUL (2011)
7. Bittl, S., Gonzalez, A.A., Heidrich, W.: Performance Comparision of Encoding Schemes for ETSI ITS C2X Communication Systems. In: VEHICULAR, pp. 58–63 (June 2014)
8. Cheng, L., Henty, B.E., Bai, F., Stancil, D.D.: Highway and Rural Propagation Channel Modeling for Vehicle-to-Vehicle Communications at 5.9 GHz. In: IEEE Antennas and Propagation Society International Symposium, pp. 1–4 (July 2008)
9. Feiri, M., Petit, J., Kargl, F.: Evaluation of Congestion-based Certificate Omission in VANETs. In: IEEE VNC, pp. 101–108 (November 2012)
10. Feiri, M., Petit, J., Schmidt, R., Kargl, F.: The Impact of Security on Cooperative Awareness in VANET. In: IEEE VNC, pp. 127–134 (December 2013)
11. Harding, J., et al.: Vehicle-to-Vehicle Communications: Readiness of V2V Technology for Application. Tech. Rep. DOT HS 812 014, Washington, DC: National Highway Traffic Safty Administration (August 2014)
12. Kargl, F., Schoch, E., Wiedersheim, B., Leinmüller, T.: Secure and Efficient Beaconing for Vehicular Networks. In: ACM VAINET, pp. 82–83 (2008)
13. 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 (November 2010)
14. Riley, G.F., Henderson, T.R.: The ns-3 Network Simulator. In: Modeling and Tools for Network Simulation, pp. 15–34 (2010)
15. Roscher, K., Bittl, S., Gonzalez, A.A., et al.: ezCar2X: Rapid-Prototyping of Communication Technologies and Cooperative ITS Applications on Real Targets and Inside Simulation Environments. In: 11th Conference WCI (October 2014)
16. Schoch, E., Kargl, F.: On the Efficientcy of Secure Beaconing in VANETs. In: ACM WiSec, pp. 111–116 (2010)
17. Schütze, T.: Automotive Security: Cryptography for Car2X Communication. In: Embedded World Conference (March 2011)