Evaluation of Congestion-based Certificate Omission in VANETs

Michael Feiri
Distributed and Embedded Security
University of Twente
The Netherlands
Email: m.feiri@utwente.nl

Jonathan Petit
Distributed and Embedded Security
University of Twente
The Netherlands
Email: j.petit@utwente.nl

Frank Kargl
Institute of Distributed Systems
University of Ulm
Ulm, Germany
Email: frank.kargl@uni-ulm.de

Abstract—Telematic awareness of nearby vehicles is a basic foundation of electronic safety applications in Vehicular Ad hoc Networks (VANETs). This awareness is achieved by frequently broadcasting beacon messages to nearby vehicles that announce a vehicle's location and other data like heading and speed. Such safety-related beacons require strong integrity protection and high reliability, two properties that are hard to combine because the communication and computation overhead introduced by security mechanisms affects reliability. This applies especially to the signatures and certificates needed for authentication.

We propose a mechanism to reduce the communication overhead of secure safety beacons by adaptively omitting the inclusion of certificates in messages. In contrast to similar earlier proposals, we control the omission rate based on estimated channel congestion. A simulation study underlines the advantages of the congestion-based certificate omission scheme compared to earlier approaches. Moreover, we show that the benefits of certificate omission outweigh the negative effect of cryptographically unverifiable beacons.

I. INTRODUCTION

In vehicular ad hoc networks (VANETs), vehicles are broadcasting beacon periodically with a frequency of 10 Hz [1]. While the upcoming European standards [2] foresee also adaptive beaconing rates between 1 and 10 Hz, we stick to the 10 Hz rate in this paper. These beacon messages are either processed directly by applications that trigger certain effects, e.g., warning the driver of a potentially imminent collision. Or vehicles use the information to build a so-called Local Dynamic Map that different applications use for purposes like traffic advise or collision warnings.

If attackers succeed to inject spoofed information into the system, this might have severe consequences, e.g., drivers misreacting due to wrong warnings. Therefore, most proposals foresee a basic integrity protection and authentication of messages based on ECDSA signatures and certificates issued by a Public Key Infrastructure (PKI) [1], [3], [4]. Thus, authorized vehicles have a private/public key pair and receive a certificate from a Certification Authority (CA) that declares the vehicle a valid participant in the VANET\(^1\). The vehicle then signs every beacon with its private key and appends the certificate to the message. Any receiver then has to verify the certificate and the signature of the beacon before further processing of the message. Therefore, security creates a communication overhead (i.e., packet size increases) and a computational overhead (i.e., time to process the packet). As was already investigated in [5]–[9], these two overheads introduce a scalability problem that can affect reliable communication and thus traffic safety in high density scenario. For example, a vehicle surrounded by 100 vehicles will receive approximately \(100 \times 10 = 1000\) messages per second and has to perform 1,000 signature verifications per second plus at maximum another 1000 certificate verifications. Beyond, the signature and certificate enlarge the beacon message by roughly 200 bytes, increasing the channel load and chance for collisions.

One proposal to deal with computational overhead is to include a dedicated cryptographic accelerator in the On-Board Unit (OBU) that can handle the approximately required 1,000 verifications per second. This approach is currently being taken by the PRESERVE project\(^2\) that designs and builds a dedicated Hardware-Security-Module (HSM) for VANETs. However, this creates additional costs and does not address the problem of communication overhead.

So [5], [6] investigated approaches to selectively skip certain steps during the communication process, e.g., by attaching certificates only to specific packets, or by skipping verification of some signatures. For instance, one could skip attaching a certificate to every packet as vehicles may cache certificates received in earlier messages. This certificate omission is the focus of this paper and was also investigated in [5]–[9].

These strategies all come at the risk that a vehicle \(A\) may receive a beacon from vehicle \(B\) without attached certificate before having cached the missing certificate of \(B\) from an earlier beacon with attached certificate. To prevent potential attackers from injecting spoofed packets, \(A\) would have to discard the beacon leading to what we term as cryptographic packet loss. If we, on the other hand, reduce the size of a lot of beacons by omitting certificates, the overall channel load, and thus also packet loss caused by collisions, will be reduced. With this paper, we want to investigate the trade-off between cryptographic- and communication-channel-induced packet loss by analyzing and comparing two of the existing schemes, namely Neighbor-based Certificate Omission

---

\(^{1}\)For simplicity, we are not addressing pseudonym schemes here

\(^{2}\)http://www.preserve-project.eu/
(NbCO) and Periodic certificate omission (POoC) schemes. Based on this, we propose a new Congestion-based Certificate Omission scheme (CbCO) that combines the advantages of NbCO and POoC.

Our main goal is to reduce overall packet loss even when the density of vehicles changes. In a simulation-based comparison to four other schemes, namely no omission, full omission, NbCO, and POoC, we show the advantages and greater flexibility of CbCO.

The paper is organized as follows: In Section II, we introduce the NbCO and POoC schemes and investigate their advantages and disadvantages and define our problem statement. Next, we introduce our CbCO scheme in Section III. Section IV presents the simulation setup, and the analysis of simulation results. Section V summarizes our findings and open issues.

II. CERTIFICATE OMISSION

Our protocol is based on the Periodic Omission of Certificates (POoC) [7]–[9] and the Neighbor-based Certificate Omission (NbCO) [5], [6]. We present those protocols in this section and discuss their advantages and disadvantages.

A. Periodic Omission of Certificates

The idea of the POoC [9] is to add the certificate every $n$ beacons.\footnote{called \textit{certificate period} in the original paper} Figure 1 gives an example with $n = 3$. The overhead reduction depends linearly on the certificate period.

But omitting certificates on a periodic schedule, creates a window of $n - 1$ beacon periods where a vehicle that has not yet cached the certificate of a sender may receive a beacon that it cannot verify and has to drop it. Assuming a beacon interval of $\Delta b$, the period until a node can verify packets from a new node in its neighborhood is $(n - 1) \times \Delta b$ in the worst case, and $\frac{(n-1) \times \Delta b}{n}$ on average. One major drawback of the POoC is that the scheme is independent of vehicle context, thus, $n$ is static. This might jeopardize safety applications. For instance, with $\Delta b = 0.1s$ and $n = 10$, a vehicle has to wait for $(10 - 1) \times 0.1 = 0.9s$ in the worst case before being capable of verifying incoming messages of vehicles that newly enter communication range (no certificate cached). At a speed of 120 km/h, this corresponds to 30 meters, too much for many safety applications. On a side note, this problem also arises whenever pseudonyms are changed.

B. Neighbor-based Certificate Omission

Schöch et al. [6] propose a different certificate omission scheme that considers the context of a vehicle in the omission decision. The idea of NbCO is to only attach the certificate to beacons if there is a change in the neighbor table. Figure 2 shows an example when a change in the neighbor table appears in the fourth beacon. A node can monitor changes to the neighbor table caused by incoming packets from unknown nodes and attach a certificate only when the neighbor table has changed since the last beacon with certificate was sent. Note that the reception of an unverifiable beacon with missing certificate also needs to trigger a neighbor table change, even if the information is unverifiable. When node $A$ is about to send a new beacon, $A$ determines if new neighbors were added to its neighbor table since the last beacon with certificate was sent. If so, a certificate is attached to the new beacon, else it is sent without certificate.

As we have found out, the main problem with the NbCO approach is that it does not scale in high density scenarios as such situations will expose a vehicle to a constantly high change of neighborhood so that almost all packets carry certificates, leading to high channel load and increased collisions.

To deal with lossy channels where the packets containing certificates for a newly arrived neighbor get lost, the authors of [6] propose that nodes could solicit for certificates if a certificate is not available within $\Delta b$ or that certificates should be attached at least every $n$ beacons.

C. Problem Statement

As discussed in the previous sections, omission of certificates in authenticated one-hop broadcast beacons is an effective way to reduce load on a communication channel. However, this improvement requires a trade-off against the immediate verifiability of messages. Some beacons may become unverifiable due to a missing certificate at the recipient, and have to be discarded. We call it \textit{cryptographic packet loss} (CPL). The more certificate omissions, the higher this cryptographic packet loss will be. Other factors that influence CPL are beacon rates and vehicle mobility.
To avoid CPL we can attach certificates to all packets, thus, going back to the basic scheme. This, however, will create larger packets, increasing channel load, and effectively leading to more packet drops because of longer packet queuing or collisions. We call this network packet loss (NPL).

The ultimate goal is to increase information awareness, i.e., the actuality of information that a vehicle has about its neighborhood. Packet loss, no matter whether caused CPL or NPL, creates additional latency until updates are received, thus decreasing information awareness. When introducing our omission scheme, we have therefore to investigate whether the induced CPL is out-weighted by the reduced NPL due to shorter messages. Then, and only then, it is reasonable to apply these strategies.

With respect to this goal, both schemes have their advantages or disadvantages. In case of a stable environment, a PoOC scheme might add too many certificates to packets, especially if \( n \) is chosen lower than necessary. On the other hand, NbCO has its limits in case of high vehicle densities and high volatility in neighborhood, as it then degenerates to the no-omission case and adds to channel congestion. While the idea to track neighborhood for omission decisions is intuitively valid, we note that in practice the behavior of this scheme is not scalable. So we argue that we need a new scheme that in addition also considers channel load as an additional factor.

Therefore, we combine the advantages of both strategies. We call our resulting approach Congestion-based Certificate Omission scheme (CbCO). Our claim is that this scheme can better address the trade-off between CPL and NPL and thus achieves better information awareness of vehicles.

### III. Congestion-based Certificate Omission Scheme

In Congestion-based Certificate Omission (CbCO), we propose to optimize omission of certificates not towards maximizing the number of omissions but instead towards minimizing the overall packet loss and thus optimizing the trade-offs between communication load and CPL. To achieve this, CbCO considers the load of the communication channel as the guiding metric. If the communication channel is free, there is no need to trade in CPL for less load on the channel. And if the communication channel is congested we want to reduce the communication load by aggressively omitting certificates. While aggressive omission increases the CPL, our evaluation shows that it will likewise decrease the overall NPL due to the reduced size of messages at an even larger rate, yielding an overall positive effect on packet loss. Figure 3 shows an example of CbCO where a congestion is detected on the third beacon. Then, the beacons 4 through 6 are transmitted without certificate.

CbCO is based on POoC and omits certificates on a periodic schedule. However, the certificate rate \( n \) at which certificates are added is flexible and triggered by the number of vehicles in communication range (as measured by the size of our neighbor table). The larger the size of the neighbor table, the larger we choose \( n \). If \( N \) is the size of the neighbor table, then \( n = \lceil \Omega(N) \rceil \), where \( \Omega \) is a weight function. This weight function defines the maximum number of omission in function of the channel occupancy. As \( \Omega \) is a key parameter of the CbCO scheme, we analyze three different trends to determine the optimal strategy. We consider \( n_{\text{max}} \) the size of the neighbor table that should trigger maximum omission and \( o_{\text{max}} \) the maximum omission rate. The selection of appropriate values for \( o_{\text{max}} \) and \( n_{\text{max}} \) is discussed in Section IV-B. We evaluate the following functions for \( \Omega \):

\[
\begin{align*}
\Omega_{\text{linear}} : y &= \min \left( \frac{x}{n_{\text{max}}} \cdot o_{\text{max}}, o_{\text{max}} \right) \\
\Omega_{\text{quad}} : y &= \min \left( \left( \frac{x}{n_{\text{max}}} \right)^2 \cdot o_{\text{max}}, o_{\text{max}} \right) \\
\Omega_{\text{trig}} : y &= \begin{cases} 
- \cos \left( \frac{\pi}{n_{\text{max}}} \cdot x \right) \cdot \frac{2o_{\text{max}}}{2} + \frac{2o_{\text{max}}}{2}, & x < n_{\text{max}} \\
0, & x \geq n_{\text{max}}
\end{cases}
\end{align*}
\]

### IV. Evaluation

To evaluate our omission scheme we focus on a city scenario with a varying number of vehicles that allow us to investigate the effects of the omission schemes especially under high communication load. While omission might not be critical at low vehicle densities, as the channel is free and can easily cope with larger packets, we expect significant effects in medium to high densities.

#### A. Simulation Setup

We use a simulation package based on JiST/SWANS [10] with extensions by Ulm University. The simulation environment provides 802.11p radio simulation and a realistic vehicular mobility model called STRAW [11], which uses map data from the U.S. Census Bureau. This simulation package allows us to efficiently simulate scenarios with a high density of vehicles [12], which is our main interest for the evaluation of congestion-based certificate omission. We use a 3 km by 3 km urban city map in Suffolk County, U.S.A., which is the same scenario as used in previous research in omission scheme [6].

In our simulation we consider only the transfer of one-hop beacon messages. While one-hop beacon messages will not

---

4 Website: http://www.vanet.info
TABLE I: Simulation parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Field size</td>
<td>3 km x 3 km</td>
</tr>
<tr>
<td>MAC</td>
<td>802.11p, 3 MBit/s</td>
</tr>
<tr>
<td>Fading</td>
<td>Rayleigh</td>
</tr>
<tr>
<td>Pathloss</td>
<td>Two-ray ground</td>
</tr>
<tr>
<td>Noise</td>
<td>Additive</td>
</tr>
<tr>
<td>Simulation time</td>
<td>60 s</td>
</tr>
<tr>
<td>Simulation runs per configuration</td>
<td>10</td>
</tr>
<tr>
<td>Transmit power</td>
<td>10.9 dB</td>
</tr>
<tr>
<td>Beaconing frequency</td>
<td>10 Hz</td>
</tr>
<tr>
<td>Payload Size</td>
<td>50 Bytes</td>
</tr>
<tr>
<td>Number of nodes</td>
<td>100, …, 1300</td>
</tr>
</tbody>
</table>

TABLE II: Cryptographic settings

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>PKAlgorithm</td>
<td>nistp256</td>
</tr>
<tr>
<td>ECC Key Type</td>
<td>compressed</td>
</tr>
<tr>
<td>Cert Size</td>
<td>140 Bytes</td>
</tr>
<tr>
<td>Signature Size</td>
<td>65 Bytes</td>
</tr>
</tbody>
</table>

be the only safety messages in the CCH, we assume that these messages will dominate the load. The configuration of the 802.11p communication channel is set to 3 MBit/s with a fixed transmission power of 10.9 dB for robust delivery of one hop safety messages [13].

The basic parameters for our simulation are in line with previous works by Schoch et.al [6] and the current draft version of IEEE 1609.2 [1]. A summary of relevant parameters is given in Table I. For the format of beacon messages we closely follow the Basic Safety Message (BSM) format as specified in SAE J2735 [14], delivered as a 45 byte DER encoded payload in a IEEE 1609.2 data message [1]. We do not consider any optional Part II attributes of the BSM format or optional parts of the 1609.2 message format. The security services specified in IEEE 1609.2 offer different options for the cryptographic additions to messages. From these options we selected the compressed representation of nistp256 keys and signatures. We do not consider certificates chains in this study. But we note that certificates chains would increase the benefit of certificate omission as the crypto payload would get even larger. A summarized description of the cryptographic additions to our simulated messages is included in Table II. Adding the 45 byte BSM and 5 byte for headers in the payload to the cryptographic material, the total size of one beacon message is 255 bytes with certificate and 115 bytes when omitting the certificate.

The beaconing rate in our simulations is fixed at 10 Hz, as recommended by SAE J2735. A full simulation run simulates 60 seconds of traffic. During this time we do not simulate pseudonym changes. We expect the rate of pseudonym changes to be low enough to not be a relevant factor for the bandwidth optimization of beaconing services.

To test the efficiency of omission schemes under high loads, we scale the number of vehicles in the simulation scenario between 100 and 1300 vehicles on a 3km x 3km road network.

On our map, this leads to an average of 5 to 68 vehicles in communication range and 18 to 252 vehicles in sensing range.

B. Analysis

For the analysis of our scheme we first investigate the settings for congestion-based certificate omission. The guiding metric we use as the foundation for congestion-based certificate omission is the number of neighbors in communication range. This metric and a basic model of a 802.11p CCH with a 10Hz BSM application on top enable us to estimate the congestion on the channel. In our simulations we identified an approximate limit of 1000 BSMs per second to saturate one communication channel in 802.11p wireless communications. We derive that 100 vehicles in communication range sending BSMs at 10Hz represent a natural limit of the communication channel.

The authenticated delivery of BSMs is a cornerstone of various safety applications. To achieve a robust delivery of verifiable BSMs, it is reasonable to consider an upper bound on the maximum number of omissions our scheme allows. As a guideline we use a recommendation in Annex B2.2 of IEEE 1609.2 v2 D12 [1] and in Annex B of ETSI TS 102637-2 draft [2]. The IEEE 1609.2 recommends to include a full chain of certificates instead of just a single certificate at least once per second. In ETSI TS 102637-2 there is a description of Cooperative Awareness Messages (CAM), which are the equivalent to BSMs in the European standardization process. There, we find a set of informative rules for context adaptive beaconing rates, which specifies a maximum time between beacon generation of one second. From this, we deduce that an interval of one second between the inclusion of a full set of authentication material should be considered as an upper bound or $n_{max} = 10$.

With the bound on the communication channel and the bound on the maximum number of omissions we have a
framework to define specific values for our CbCO scheme. Figure 4 shows the resulting $\Omega$ functions for $o_{\text{max}} = 10$ and $n_{\text{max}} = 100$.

While the linear function is a simple baseline to scale the number of omissions directly related to the number of neighboring vehicles, the other functions reduce the omission rate at lower vehicle densities to prevent CPL when there is no direct benefit in reduced NPL. We generally want to keep the number of omission low until the channel needs to counter increasing NPL. For this reason we propose two additional ways to calculate the number of omissions. A quadratic function lets the number of omissions grow slower in less densely connected environments. And a trigonometric function produces similarly slow growth of omissions on sparsely connected environment while accelerating the increase of omissions more aggressively in densely populated environments.

To assess the quality of our CbCO, we analyze the number of omissions and the amount of collision based on CPL. Figure 5 shows the average percentage of beacons sent with a certificate attached to it. This is the inverse of the average number of omissions. We see the linear and trigonometric curves closely matching each other, while the quadratic calculation of omissions results in less omissions.

Next, we want to investigate the consequences of these different functions in terms of omissions. We measure this as cryptographic packet loss, i.e. the relative number of unverifiable messages that are dropped, and then the receiver misses a certificate to verify them. This is shown in Figure 6. We see that again the linear and trigonometric curves match quite closely, while the quadratic method results in fewer unverifiable messages.

In practice we have to consider a secondary effect of omitting certificates. The goal of certificate omissions is to reduce the load on the network in order to have fewer collisions and thus fewer packet loss. To see this effect we calculate a baseline of successful message delivery without any inclusion of any certificates. Using this baseline we can calculate the added packet loss due to the inclusion of certificates. Since different omissions schemes result in different numbers of omissions we see different characteristics for each scheme.

The graph in Figure 7 shows the average increase in network packet loss (NPL) relative to packets without certificates. As a reference, we also show the additional packet loss for no omissions (NoOm). As one can see, CbCO achieves a significantly reduced packet loss due to reduced message size compared to the NoOm scheme. One can also see that the quadratic $\Omega$ function performs a little worse than the two other.

Our goal is to decrease overall packet loss, considering NPL and CPL. This is shown in Figure 8. First of all, we can again observe the benefits of the omission schemes compared to attaching certificates to all packets. There is also a slight
Fig. 8: Increase of packet loss due to inclusion of certificates for different variants of CbCO, counting NPL + CPL

Fig. 9: Illustration of the effect of counting cryptographic packet loss as regular packet loss

Fig. 10: Average number of unverifiable beacons until arrival of certificate

Fig. 11: Maximum number of unverifiable beacons until arrival of certificate

The advantage of the linear and trigonometric $\Omega$ functions. Additionally, we note that above 1000 vehicles, we see the effect of the bounding of omissions, as the different $\Omega$ functions converge. Figure 9 illustrates the composition of network packet loss and cryptographic packet loss using CbCO-linear as an example. So while CbCO introduces additional CPL, it is evident that the saved NPL outweighs this by far. However, we still need to investigate whether this comes at the expense of increased latency until a communication partner receives the certificate required to start authenticating messages.

Figures 10 and 11 illustrate the average and maximum number of unverifiable beacons until arrival of the certificate. As for the number of omissions, we notice that the quadratic method has a lower latency until messages become verifiable. We note that the linear way to calculate the congestion-based omission seems to provide a slightly improved latency characteristic compared to the trigonometric function.

We conclude that the linear and trigonometric approaches perform very similar, with slight advantages for the linear approach. We consider the advantage of the linear approach to be rooted in the faster increase of omissions in situations with high connectivity. These situations generally have more impact on the simulation results and keeping the number of omissions down until the channel is overloaded is an effective approach. The quadratic function shows the limit of following this line of thought. We see the advantage for the quadratic approach in the latency until a message becomes verifiable. Finally we remark that the quadratic scheme showed a slightly worse overall increase of packet loss compared to the other approaches.
C. Comparison

To assess the utility of congestion based certificate omission schemes, we conduct comparisons to the previously proposed omission schemes. We select Periodic Omission of Certificates (POoC) as described in [9], using the parameter $\alpha = 10$, and Neighbor-based Certificate Omission proposed in [6]. Where applicable we also compare the schemes against a baseline of having no certificate omissions at all. An overview of the schemes is given in Table III.

The basic percentage of certificates included in messages is an indicator of the performance of each scheme. In Figure 12 we remark that the congestion based omission scheme is converging to the same 90% omission rate as the POoC-10 scheme. On the other hand, the neighbor-based certificate omission scheme reduces omissions in densely populated scenarios due to the increased amount of neighbor changes in the network. This of course helps to keep down the CPL for the NbCO scheme, as can be seen in Figure 13. But the price for this low amount of CPL is a much higher amount of regular CPL due to collisions in the communication channel as can be seen in Figure 14. All values are again relative to a baseline where we do not attach certificates at all (for NPL) or where every packet is assumed to be verifiable (for CPL). We note that the POoC scheme on the other hand performs well in terms of minimizing network packet loss but shows problems with regard to cryptographic packet loss.

Finally, Figure 15 presents an amortized total results for packet loss induced by certificate inclusion. In this graph we consider unverifiable packets to be cryptographic packet loss and see that the congestion based omission schemes deliver the best scalability in this overall view on the communication performance.

V. CONCLUSION AND FUTURE WORK

We investigated the problem of scalability of security mechanisms in VANETs, especially with respect to communication overhead created by attaching certificates to all messages. Following earlier proposals, we suggest to adaptively omit certificates when sending beacons to reduce the channel load based on a Congestion-based Certificate Omission scheme (CbCO). This scheme uses an estimate of the channel congestion to decide whether to omit certificates. Using a simulation study, we investigate if the number of neighbors can be used to control the omission rate. The use of omission schemes leads to cryptographic latency due to intermittently missing certificates or even cryptographic packet loss if we consider unverifiable packets to be useless. Simulation results show that CbCO achieves a good balance between this effect and overall packet loss due to large messages. This shows that our scheme reduces the overall packet loss compared to the standard security mechanism that does not use certificate omission. Furthermore, we have shown that our schemes adapts better to varying vehicle densities than previous proposals.

As future work, we envision a cross-layer scheme in order to use more direct information about congestion in communication channels. This could be part of a larger effort to improve the overall quality of service in secure communication systems. Security components in communication systems can and should use cross layer information to make better decisions about security trade-offs while preserving a general separation.
results strongly suggest the consideration and adoption of adaptive beaconing rates on the behavior of CbCO. Adaptive beaconing rates in particular represent a higher level omission of concerns. In this context we also propose to analyze the impact of higher bandwidths, adaptive beacon sizes and adaptive beaconing rates on the behavior of CbCO. Adaptive beaconing rates in particular represent a higher level omission scheme for entire beacons and it is necessary to investigate the effects of using omission schemes concurrently on multiple layers. While we see still some room for improvement, our results strongly suggest the consideration and adoption of certificate omission in IEEE and ETSI standards.

ACKNOWLEDGEMENTS

The research leading to these results has received funding from the European Union’s Seventh Framework Programme project PRESERVE under grant agreement n°269994.

REFERENCES