Congestion-based Certificate Omission in VANETs

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

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

Frank Kargl
Institute of Distributed Systems
University of Ulm
Ulm, Germany
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.

Categories and Subject Descriptors

C.2.0 [**Computer-Communication Networks**]: General

Keywords

VANET, security, certificate omission, congestion

1. INTRODUCTION

In vehicular ad hoc networks (VANETs), vehicles periodically broadcast beacon messages with a frequency between 1 and 10 Hz. These beacon messages are then either processed directly by applications to 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.

Our main goal is to reduce the loss of beacon messages due to attached authentication data by adaptively omitting certificates. In a simulation-based comparison to previously proposed schemes we show the advantages and greater flexibility of Congestion-based Certificate Omission (CbCO).

VANET'12, June 25, 2012, Low Wood Bay, Lake District, UK.
ACM 978-1-4503-1317-9/12/06.

2. CERTIFICATE OMISSION

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 this *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).

Our 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 by CPL or NPL, creates additional latency until updates are received, thus decreasing information awareness. When introducing our omission scheme, we therefore have 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 omission strategies.

With respect to this goal, existing schemes have their advantages and drawbacks. In case of a stable environment, a protocol based on the Periodic Omission of Certificates (POoC) [2] might add too many certificates to packets, especially if n is chosen lower than necessary. On the other hand, Neighbor-based Certificate Omission (NbCO) [3] 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. We argue that we need a new scheme that also considers channel load as an additional factor.

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

3. CONGESTION-BASED CERTIFICATE OMISSION SCHEME

In Congestion-based Certificate Omission (CbCO), we propose to optimize omission of certificates not towards maxi-

Figure 1: Example of CbCO

mizing the number of omissions but instead towards minimizing the overall packet loss and thus optimizing the tradeoffs 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 1 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 $n = \lfloor \Omega(N) \rfloor$, where Ω is a weight function. Considering n_{max} the size of the neighbor table that should trigger maximum omission and o_{max} the maximum omission rate, we investigated the following Ω functions:

$$\Omega_{linear} : y = \min\left(\frac{x}{n_{max}} \cdot o_{max}, o_{max}\right) \quad (1)$$

$$\Omega_{quad} : y = \min\left(\left(\frac{x}{n_{max}}\right)^2 \cdot o_{max}, o_{max}\right) \quad (2)$$

$$\Omega_{trig} : y = \begin{cases} -\cos\left(\frac{\pi}{n_{max}} \cdot x\right) \cdot \frac{o_{max}}{2} + \frac{o_{max}}{2}, & x < n_{max} \\ o_{max}, & x \geq n_{max} \end{cases} \quad (3)$$

4. 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.

The basic parameters for our simulation are in line with previous works by Schoch et.al [3] and the current draft version of IEEE 1609.2 [1]. A summary of relevant parameters is given in Table 1.

Table 1: Simulation parameters

Parameter	Value
Field size	3 km × 3 km
MAC	802.11p, 3 MBit/s
Beaconing frequency	10 Hz
Payload Size	50 Bytes
Number of nodes	100, . . . , 1300
Key Type	nistp256, compressed
Cert Size	140 Bytes
Signature Size	65 Bytes

Table 2: Omission Schemes

Name	Options	Abbreviaion
Periodic Omission [2]	$\alpha = 10$	POoC-10
Periodic Omission [2]	$\alpha = 3$ [3]	POoC-3
Neighbor-based [3]	-	NbCO
Congestion-based	Linear	CbCO-linear
Congestion-based	Quadratic	CbCO-quad
Congestion-based	Trigonometric	CbCO-trig
No omissions	-	NoOm

The basic percentage of certificates included in messages is an indicator of the performance of each scheme. In Figure 2 we see that our congestion based omission schemes converge 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 keeps down the CPL for the NbCO scheme. But the price for this low amount of CPL is a much higher amount of regular NPL due to collisions in the communication channel as can be seen in a comparison of pure NPL in Figure 3 and the combination of NPL and CPL in Figure 4. The values in these figures show the increase of packet loss relative to a baseline of not attaching any certificates at all. We note that all described schemes induce less packet loss than adding authentication data to beacons without any omissions (NoOm), even when considering cryptographic unverifiability as CPL.

The Congestion-based Certificate Omission scheme offers a balance between minimizing cryptographic packet loss and network packet loss. The variant of CbCO using the linear method to compute the number of omissions appears as the best trade-off between the two types of packet loss. Using an adaptive mechanism to adjust the omission of certificates can scale as well as the non-adaptive POoC scheme, while providing better characteristics to reduce cryptographic latency and cryptographic packet loss. Compared to the NbCO, CbCO offers clearly superior overall scalability in highly congested scenarios. The idea of using the network context to define the number of omissions seems useful. Unfortunately, the event based approach of NbCO to maximize certificate omission while optimizing cryptographic packet loss does not scale. Calculating certificate omission on neighborhood change leads to fewer omissions and consequently enlarged message sizes in exactly the situations when we want to take load off of the communication channel.

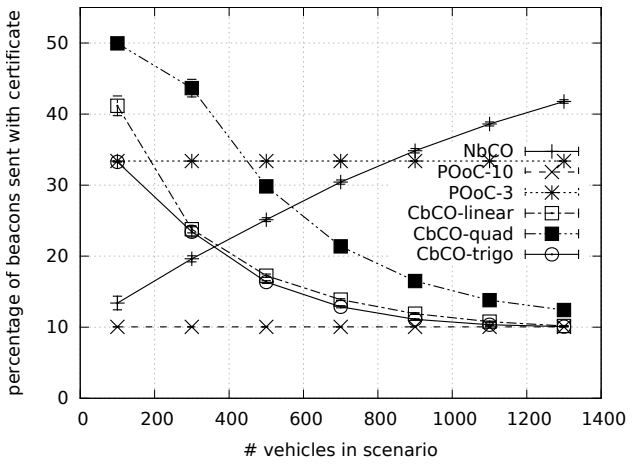

Figure 2: Average percentage of certificate omission in other protocols

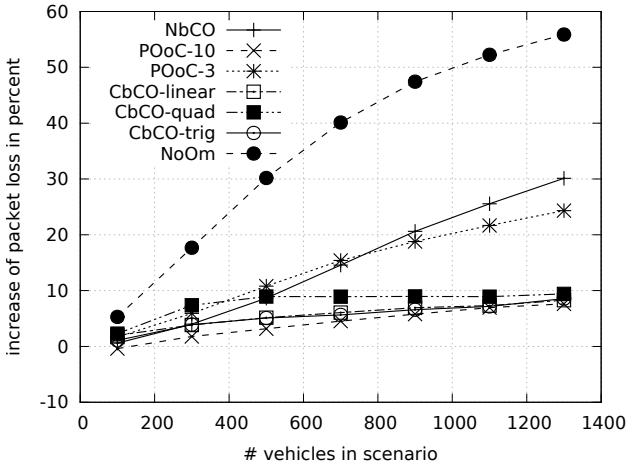

Figure 3: Increase of packet loss due to inclusion of certificates (NPL only)

5. 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

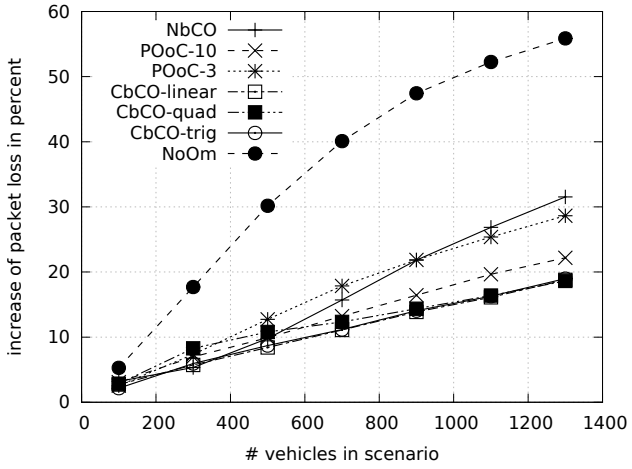

Figure 4: Increase of packet loss due to inclusion of certificates (NPL + CPL)

certificate omission. Furthermore, we have shown that our schemes adapts better to varying vehicle densities than previous proposals.

As future work, we first envision a cross-layer scheme in order to use less indirect 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 of concerns. In this context we secondly propose to analyze the impact of an adaptive beaconing rate on the behavior of CbCO. Adaptive beaconing is essentially 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.

6. ACKNOWLEDGEMENTS

The research leading to these results has received funding from the European Union's Seventh Framework Programme project PRESERVE under grant agreement № 269994.

7. REFERENCES

[1] IEEE Draft Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages. *IEEE P1609.2/D12, January 2012*, pages 1 – 266.

[2] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy. On the performance of secure vehicular communication systems. *Dependable and Secure Computing, IEEE Transactions on*, 8(6):898 –912, nov.-dec. 2011.

[3] E. Schoch and F. Kargl. On the efficiency of secure beaconing in vanets. In *Proceedings of the third ACM conference on Wireless network security*, WiSec '10, pages 111–116, New York, NY, USA, 2010. ACM.