Formal Model of Certificate Omission Schemes in VANET

Michael Feiri*, Jonathan Petit*‡, Frank Kargl*†
*Services, Cybersecurity and Safety, University of Twente, The Netherlands
†Institute of Distributed Systems, University of Ulm, Germany
‡Department of Computer Science, University College Cork, Ireland

***Abstract*—The benefits of certificate omission schemes in VANET have been so far proven by simulation. However, the research community is lacking of a formal model that would allow implementers and policy makers to select the optimal parameters for such schemes. In this paper, we lay the foundations of the formal model for certificate omission schemes in VANET. We apply the model to 'No Omission' and 'Periodic Omission', which validates the previous simulation and formulates the optimal parameters for these schemes.**

***Keywords*—Analytical model, security, certificate omission, VANET.**

I. Introduction

Vehicular ad-hoc networks (VANET) enable vehicles to periodically broadcast position beacons, thus providing telematic awareness to neighboring vehicles. The impact of Vehicle-to-X communication (V2X) on safety and traffic efficiency makes security mandatory. Therefore, to prevent injection of messages by external attackers, each vehicle 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. Hence, security creates a communication overhead (i.e., packet size increases) and a computational overhead (i.e., time to process the packet). One approach to reduce overhead is to omit certificates, decreasing the beacon packet size by 140 bytes [1]. Benefits of the certificate omission schemes described below were proven by simulation in [2], [3], [4].

- No omission of certificates (NoOm): This scheme serves as a baseline as it performs no omission.
- Periodic omission of certificates (POoC) [5]: The idea of POoC is to include a certificate, followed by $n-1$ omissions, resulting in a periodical pattern of length n.
- Neighbor-based certificate omission (NbCO) [6]: This scheme 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.
- Congestion-based certificate omission (CbCO) [3]: This scheme considers the load of the communication channel as the guiding metric. If the communication channel is free, there is no need to omit certificates. If the channel is congested, the communication load is reduced by aggressively omitting certificates.

However, a formal model is needed to analytically prove which scheme is best-suited for VANET, and identify its optimal parameters (e.g., n). The main contribution of this paper are the description of the formal model and its application to NoOm and POoC.

The rest of the paper is organized as follows. Section II presents the system model used for the formal model. Section III shows the preliminary results of NoOm and POoC. Section IV outlines the future work required to define the full analytical model in order to find the optimal parameters for certificate omission scheme.

II. System Model

The goal of modeling certificate omission formally is to analytically investigate the effect on packet delivery under consideration of cryptographic packet loss. Cryptographic packet loss (CPL) in this context is defined as discarding signed messages that can not be verified cryptographically due to lack of the senders certificate [3]. Without the senders certificate it is impossible to verify the trust relationship between the sender and a trusted certification authority, which is the expected trust model for secure vehicular broadcast communication. We refer to other forms of packet loss, due to classic signal propagation effects, as network packet loss (NPL).

Packet delivery success generally depends on a multitude of factors such. Such factors can be the distance between sender and receiver, the payload length of messages, the load on the communication channel, shadowing and reflection of signals, or environmental aspects such as line of sight. To remain independent of the intricacies of signal propagation details in specific scenarios, we restrict our assumptions about the communication channel to an abstract packet delivery probability function $D_s(d)$ for a given scenario s with the distance d between sender and receiver as input. This function incorporates averaged consideration of above mentioned attributes such as payload length and channel load, including the the averaged effects of the selected omissions scheme on these attributes.

Certificate omission achieves lower NPL through a reduction of load in the communication channel. This is obviously a trade-off against potential CPL. However this CPL effect is only present until the first reception of the certificate of a sender. Therefore we want to quantify the time until the first reception of the certificate of a vehicle with an unknown cryptographic identity. This can occur because a vehicle arrives within communication range for the first time or because

978-1-4799-7660-7/14/$31.00 ©2014 IEEE

a vehicle switched its cryptographic identity for reasons of privacy protection.

The predominant communication pattern in vehicular communication is expected to be the exchange or position beacons, known as CAM or BSM in the ETSI ITS and IEEE 1609 families of standards. These beacons are expected to be sent at a fixed frequency of 10Hz. We use this regular schedule to establish a baseline metric of beacon periods, which represents 100 milliseconds of time. This beacon period allows us to analyze network effects based on rounds of message exchanges.

Finally we combine the model for the expected time until the first reception of a vehicles certificate (CPL) with the general NPL packet loss. This yields the packet reception probability at the receiver side under consideration of CPL and NPL for a scenarios packet delivery probability $D_s(d)$ as a function of beacon periods and distance between sender and receiver.

III. Preliminary Results

Without loss of generality we select two representative examples of $D_s(d)$ based on the packet delivery properties of the 802.11p subsystem in the JiST/SWANS simulation package with extensions from the University of Ulm. We use two scenarios to illustrate our analytical model:

- No congestion: A scenario with two vehicles communicating in a 802.11p channel with default settings. No other vehicles introduce noise or packet loss in this scenario. Only signal propagation effects reduce packet delivery success over longer distances between the two vehicles.
- High congestion: A scenario that uses a backdrop of a high load on the communication channel, produced by vehicles using the same communication pattern as the sender and receiver vehicles under investigation, i.e. NoOm or a variant of POoC. By projecting a 1 km^2 scenario with 260 vehicles on a $\sqrt{2}$ km one-dimensional line we replicate a simplified high congestion scenario as suggested in [7]. We extend the scenario in each direction by the length of the maximum sensing range with the same vehicle density to ensure equal congestion in the center of the scenario.

Figures 1 and 2 show the packet delivery rates for the selected example scenarios. Each certificate omission scheme results in different channel congestion due to differing lengths of messages causing some diversification. Figures 3 and 4 show polynomial curve fitting applied to the simulated values to arrive at smooth distribution curves. This represents the baseline for packet delivery success (NPL only) in our illustrative examples.

The delivery rate function $D_s(d)$ and thus the NPL model do account for the effect of payload sizes in a scenario. This implicitly includes the effect of the selected certificate omission protocol on channel load. Next we want to derive the explicit probability of successfully receiving a message with an included certificate. We derive this from the overall message delivery success rate multiplied by the rate of certificate inclusion, which we introduce as the discrete value c.

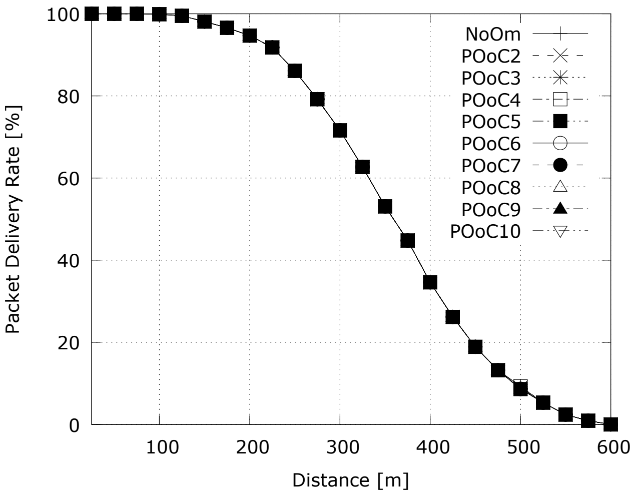

Fig. 1. Packet delivery rates without load on the communication channel

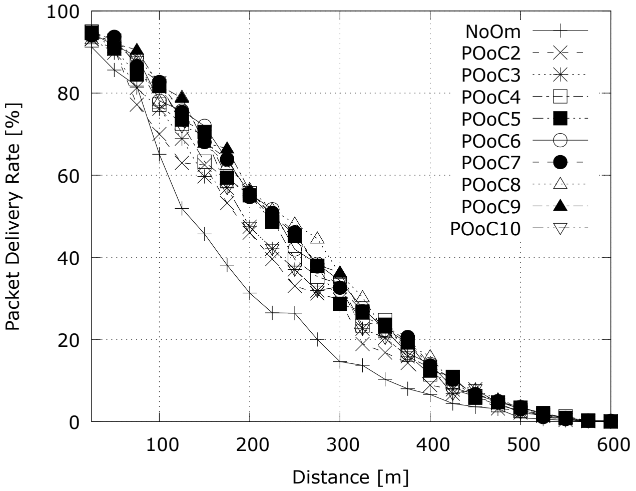

Fig. 2. Packet delivery rates with high load on the communication channel

$$D_s(d) * c \tag{1}$$

For example, in the case of POoC3 we omit the certificate two times followed by one inclusion, leading to an inclusion rate of 1/3. Figures 5 and 6 show the resulting graphs for the example scenarios and the investigated omission schemes. The graph of NoOm is unchanged compared to the previous figures, as the certificates are always included.

As the probability of receiving a certificate is known, we can derive the probability of reception of a certificate within a given number of beacon periods. This defines the extent of CPL that is introduced by certificate omission. We consider the probability of receiving a certificate within any of up to n beacon periods as the inverse of the probability to not receive any certificate within n beacon periods. We start with the probability of not receiving a certificate within one beacon period, which is

$$1 - D_s(d) * c \tag{2}$$

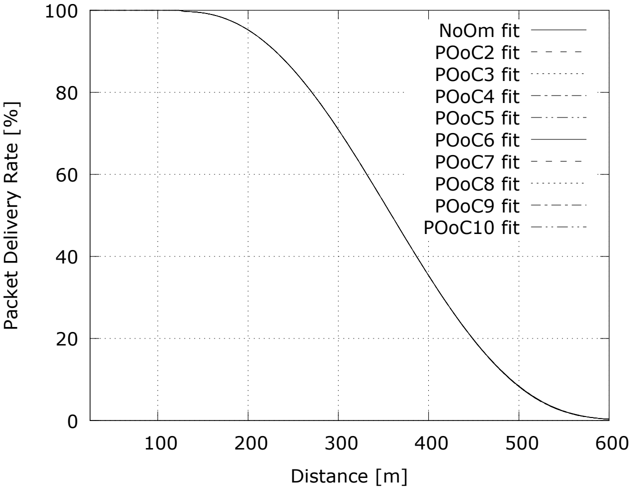

Fig. 3. Polynomially fitted packet delivery rate without load on the communication channel

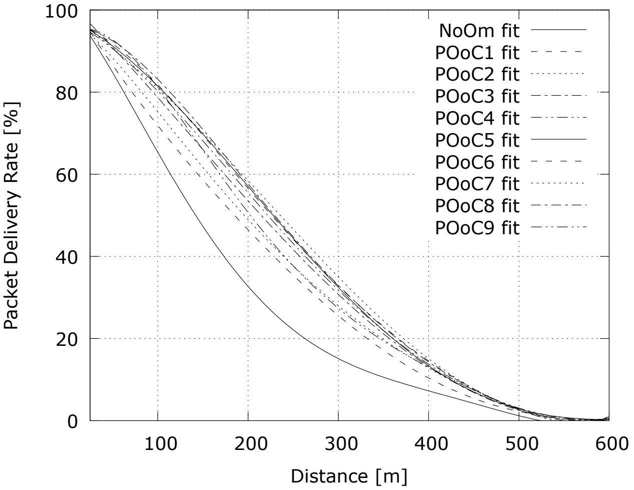

Fig. 4. Polynomially fitted packet delivery rate with high load on the communication channel

Taken to the power of n, we get the probability that no certificate is received in any of n beacon cycles. The inverse of this is then the probability that a certificate is included one or more times in n beacon cycles. Thus we get the probability of having received a certificate within n beacon periods as

$$1 - ((1 - D_s(d) * c)^n) \tag{3}$$

We now have two free variables d and n. To show an example as a two-dimensional graph we fix $d = 300$. The resulting graphs for the probabilities of receiving a certificate within n beacon periods are shown in Figures 7 and 8

Finally, we can now combine the probability of having received a certificate (CPL) with the probability of receiving a packet at all (NPL). The multiplication of these probabilities gives the overall probability of successful packet transfer under consideration of both sources of packet loss.

$$(1 - ((1 - D_s(d) * c)^n)) * D_s(d) \tag{4}$$

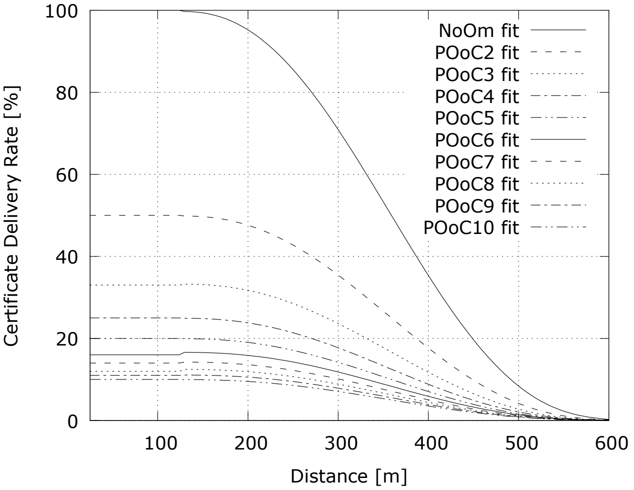

Fig. 5. Certificate delivery rate without load on the communication channel

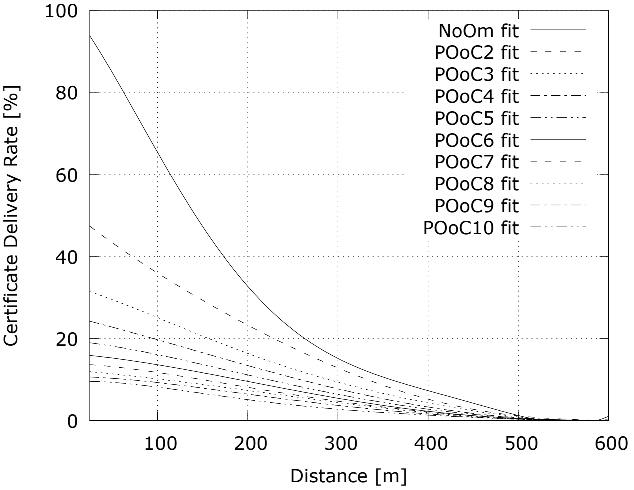

Fig. 6. Certificate delivery rate with high load on the communication channel

Figures 9 and 10 show the overall packet delivery rates for the two sample scenarios, at the reference distance of 300 m between sender and receiver. In Figure 9 we see how all schemes converge to the same ideal packet delivery success rate if there is no congestion. Certificate omission in this scenario only introduces down-sides without any improvements. Figure 10 however shows more diverse results. Certificate omission schemes converge to different packet delivery rates after the initial probability of CPL subsides. The speed of reducing CPL and the convergence to higher overall packet delivery success values give certificate omission schemes an advantage over not performing certificate omission.

IV. Conclusion and Future Work

In this work we developed an analytical model to predict packet delivery probabilities for secure broadcast communication in vehicular networks under consideration of cryptographic packet loss. The results are in line with simulation models that have served as validation for the introduction of omission schemes in previous works.

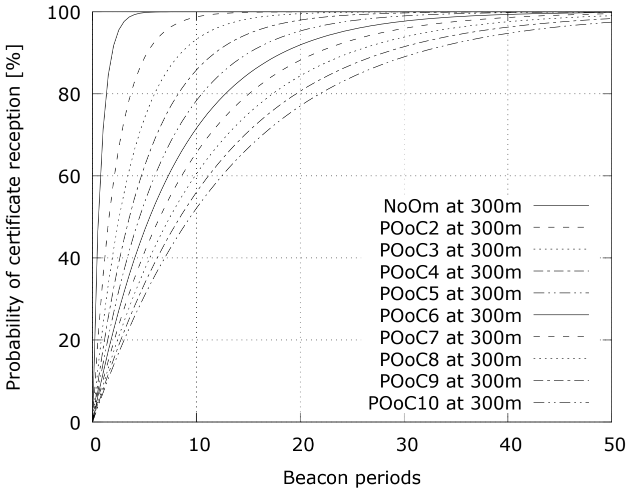

Fig. 7. Probability of certificate reception after n beacon periods without load on the communication channel at 300m distance

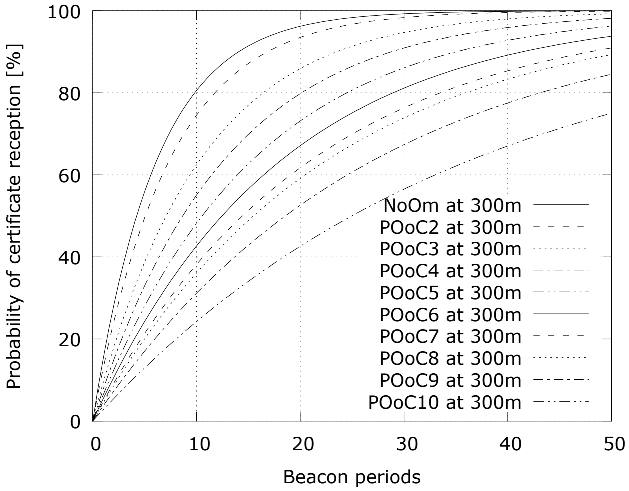

Fig. 8. Probability of certificate reception after n beacon periods with high load on the communication channel at 300m distance

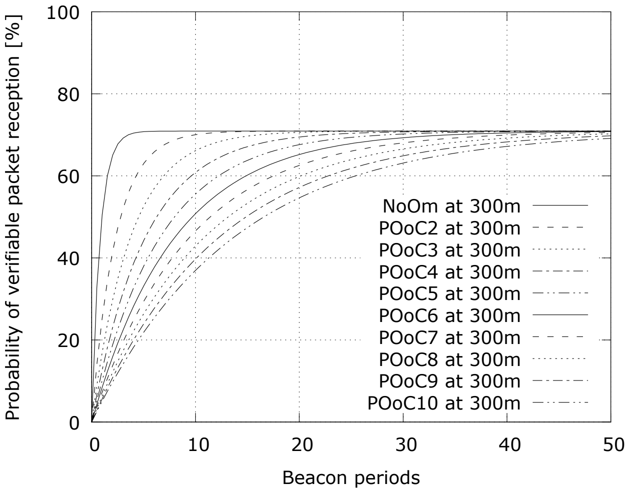

Fig. 9. Overall packet delivery rate considering CPL and NPL without load on the communication channel at 300m distance

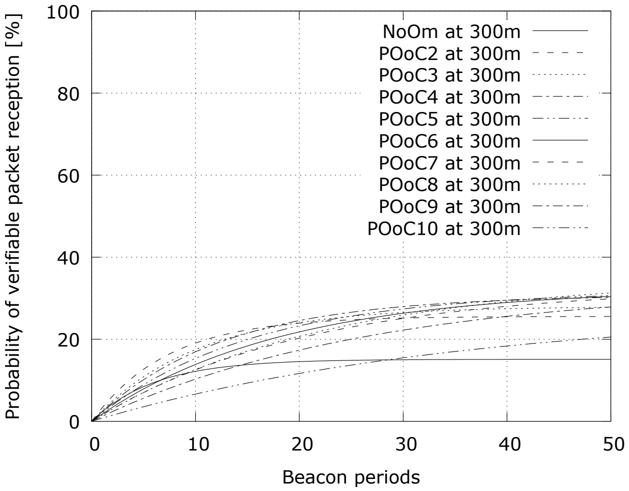

Fig. 10. Overall packet delivery rate considering CPL and NPL with high load on the communication channel at 300m distance

The model in this paper only considers the NoOm and POoC omission schemes. Alternative omissions schemes, such as CbCO and NbCO, rely on context sensitive mechanisms. Building models for such schemes remains as future work. Furthermore the model can be enhanced by considering variations of relevant attributes such as variable payload length in more detail. The availability of precise analytical models for omission schemes is expected to enable selection of schemes and parameters with the most beneficial attributes.

Acknowledgement

This work received funding from the European Union's Seventh Framework Programme project PRESERVE under grant agreement no. 269994.

References

[1] ETSI TC ITS, "ETSI TS 103 097 v1.1.1 - intelligent transport systems; security header and certificate formats," Standard, TC ITS, 2013.

[2] M. Feiri, J. Petit, and F. Kargl, "Congestion-based Certificate Omission in VANETs," in *Ninth ACM International Workshop on Vehicular Ad Hoc Networks (VANET '12)*, June 2012, pp. 135–138.

[3] ——, "Evaluation of Congestion-based Certificate Omission in VANETs," in *Fourth IEEE Vehicular Networking Conference (VNC '12)*, November 2012, pp. 101–108.

[4] M. Feiri, J. Petit, R. K. Schmidt, and F. Kargl, "The impact of security on cooperative awareness in VANET," in *Fifth IEEE Vehicular Networking Conference (VNC '13)*, December 2013, pp. 127–134.

[5] 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, nov.-dec. 2011.

[6] E. Schoch and F. Kargl, "On the efficiency of secure beaconing in VANETs," in *Third ACM conference on Wireless network security (WiSec '10)*, March 2010, pp. 111–116.

[7] R. K. Schmidt, A. Brakemeier, T. Leinmüller, F. Kargl, and G. Schäfer, "Advanced carrier sensing to resolve local channel congestion," in *Proceedings of the Eighth ACM international workshop on Vehicular inter-networking*. ACM, 2011, pp. 11–20.