Efficient Authorization Authority Certificate Distribution in VANETs

Sebastian Bittl and Karsten Roscher
Fraunhofer ESK, Munich, Germany

Keywords: Certificate Distribution, VANET, Security.

Abstract: Car-to-X communication systems are about to enter the mass market in upcoming years. Security in these networks depends on digital signatures managed by a multi-level certificate hierarchy. Thereby, certificate distribution is critical in regard to channel utilization and data reception delay via security caused packet loss. These issues are even more significant in case not only pseudonym certificates but also authorization authority certificates have to be exchanged between nodes in the VANET. Prior work has not studied distribution of the elements of a multi-level certificate chain in detail. Hence, this work provides an analysis of the currently standardized mechanisms and identifies several drawbacks of the straight forward solution proposed so far. Thereby, we find a severe denial of service attack on that solution. Moreover, the distribution problem is found to be similar to the packet forwarding problem encountered in position-based routing. Thus, we study several strategies for efficient distribution of a certificate chain in regard to channel load, which are adapted from their counterparts in position-based routing. Thereby, we find that by combining pseudonym certificate buffering with requester based responder selection the requirement for certificate chain distribution in VANETs can be removed completely. Hence, the proposed design avoids the identified denial of service weakness and reduces the worst case size of the security envelope of VANET messages by more than a third.

1 INTRODUCTION

Vehicular ad-hoc networks (VANETs) based on wireless Car-to-X communication are about to enter the mass market in upcoming years. In both Europe and the USA important progress is being made within the European Telecommunications Standards Institute Intelligent Transport Systems (ETSI ITS) and Wireless Access in Vehicular Environments (WAVE) frameworks (MoU, 2011; Harding et al., 2014). Security of these systems is a core point of concern, as their main use cases are safety critical advanced driver assistance systems (ADAS). Thus, a security approach based on digital signatures managed via a multi-level certificate hierarchy has been developed.

For ETSI ITS, the certificate hierarchy consists of three levels. These are given by the root certificate(s) authorizing so called authorization authority certificates (AACs), which are used to authorize pseudonym certificates (PSCs, also called authorization tickets) (103, 2015). Thus, an authorization authority acts as a certificate authority. WAVE does not limit the number of certificate hierarchy levels, but the minimum amount is three. PSCs are used to sign an ITS-station's (ITS-S's) messages, e.g., Cooperative Awareness Messages (CAMs) or Basic Safety Messages (BSMs). To verify messages, the receiver needs to know about the certificate chain of the receiver. In order to avoid tracking of vehicles pseudonym certificates are changed rapidly by each ITS-S. Thus, it is necessary to exchange certificates, except of the root certificate(s) known to all stations, on demand between participants in the VANET.

It has been shown that the overhead in message size by certificate distribution leads to increased channel load, which can significantly decrease VANET system performance (Kargl et al., 2008). Thus, bandwidth efficient strategies for certificate distribution are required. Nonetheless, recent work has focused on distribution strategies of PSCs. In contrast, AAC distribution, as required by a hierarchical certificate chain approach, has not gained much attention so far.

A completely centralized scheme distributing all certificate authority (CA) certificates to all ITS-S from a back bone network, without ITS-S to ITS-S dissemination, is described in (Morogan and Muftic, 2003). To avoid dependence on such back bone network distribution, which would also require cooperation of all CAs, both ETSI ITS and WAVE use a decentralized scheme. Thereby, an AAC is distributed by all ITS-S using it, similar to the distribution of ITS-S's individual PSCs (103, 2015; WAV, 2013).

Bittl, S. and Roscher, K.
Efficient Authorization Authority Certificate Distribution in VANETs.
DOI: 10.5220/0005685600850096
In *Proceedings of the 2nd International Conference on Information Systems Security and Privacy (ICISSP 2016)*, pages 85-96
ISBN: 978-989-758-167-0

The maximum size of the security envelope added at the network layer of VANETs greatly influences overall system design. It limits the size of higher layer data sets, as the size of packets which can be handed over to the lower level access layer is limited. Increasing this limit is unsuitable, as this would significantly deteriorate overall system performance, e.g., due to an increase in collisions on the wireless channel.

AAC exchange between ITS-Ss in VANETs following ETSI ITS and WAVE standards is specified in (103, 2015; WAV, 2013). However, we find that the straight forward approach for certificate chain dissemination taken there can lead to significant peaks in channel load. Moreover, the maximum size of the security envelope gets increased significantly by more than a half compared to the preceding standard version using only PSC distribution (103, 2013; 103, 2015). This is because an included certificate accounts for more than 50% of the size of the entire security envelope (Bittl et al., 2015b).

Moreover, the specified request mechanism for AACs can be (mis-)used by an attacker to perform a serious denial of service (DOS) attack on the VANET. Thus, we propose an alternative AAC distribution strategy. It combines multiple concepts like temporary buffering of unauthorized PSCs and AAC emission strategies inspired by packet forwarding algorithms taken from position-based routing (often called GeoNetworking within ETSI ITS).

The remainder of this work is outlined as follows. At first, Section 2 provides a review of prior work. Afterwards, Section 3 defines the problems addressed in this work. New concepts for efficient AAC distribution are introduced in Section 4. An evaluation of the proposed concepts is provided in Section 5. Lastly, a conclusion about achieved results is given in Section 6 together with possible topics of future work.

2 RELATED WORK AND ATTACKER MODEL

This section provides a review of related work and introduces the assumed attacker model.

2.1 Related Work

Security mechanisms within ETSI ITS and WAVE use digital signatures to secure authenticity and integrity of messages. Required parameters, e.g., public keys, are contained in certificates, which are part of a multi-hierarchy certificate chain. Thereby, a low number of cross-signed root certificates acts as the common anchor of trust, provided to ITS-Ss during manufacturing. Manufacturers of ITS-Ss, e.g., inside vehicles or road side units (RSUs), also equip their devices with their individual AAC alongside with PSCs.

AACs are used to secure PSCs, while PSCs are used to sign sent messages. The used PSC is changed frequently to avoid vehicle tracking. To enable realtime secured communication, participating ITS-S have to exchange their corresponding AACs as well as PSCs (103, 2015; Task Force PKI, WG Security C2C-CC, 2012; 102, 2012a). Otherwise, receivers cannot verify messages, which leads to so called cryptographic packet loss, i.e., dropping of messages.

Both ETSI ITS and WAVE do not use dedicated messages for certificate distribution. Instead, sporadic piggybacking of such data on higher level messages, e.g., cyclically sent CAMs or BSMs, is used. Explicit and implicit requests are used for PSCs dissemination as studied in (Bittl et al., 2015a). In contrast, only explicit requests are used for AACs. This is done to keep the amount of transmissions of the certificate chain low, as thereby the AAC is emitted together with the currently used PSC. The overhead caused by including a certificate into the so called security envelope of a message is quite significant, almost doubling the size of the whole message (Bittl et al., 2015b; 103, 2015). Thus, inclusion of PSC and AAC into the security envelope increases a message's size by a factor of almost three. As many ITS-Ss share the same AAC, e.g., all cars from the same manufacturer, exchange of this information can be expected to happen with a much lower frequency then those of PSCs being individual to each ITS-S.

To the best of our knowledge, no detailed study on AAC, or the general case of a multi-hierarchy certificate chain, distribution within current VANET approaches has been published so far. Closest related work proposes a centralized distribution scheme for all CA certificates in VANETs (Morogan and Muftic, 2003), an approach not used in current VANET standards (103, 2015; WAV, 2013).

Instead of studying hierarchical certification schemes, prior work focused on decentralized CAs residing within the VANET itself (Masdari and Barbin, 2012; Sen et al., 2007). However, such schemes do not provide the high level of security provided by infrastructure based CAs (Masdari and Barbin, 2012).

An illustration of a message sequence exchanged between two ITS-Ss A and B causing an AAC request according to (103, 2015) is given in Figure 1. Mechanisms within WAVE are very similar. For a more compact presentation, we stick to ETSI ITS notation.

Due to the various inclusion rules of PSCs into CAMs it is also possible that the first message from B received at A contains the PSC, e.g., due to cyclic

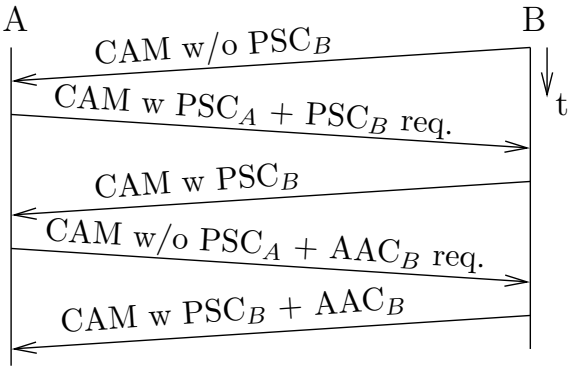

Figure 1: Message sequence leading to an AAC request.

inclusion of PSCs into CAMs. However, in both cases an AAC request can only happen after station A has already received the PSC of B (called PSC$_B$ in Figure 1). This feature is used in the system optimization approach suggested in Section 4.4.

An interesting finding is that requesting of AACs shows similarities to multi-hop forwarding in position-based routing (e.g., so called GeoNetworking in ETSI ITS). In both cases an ITS-S (security: responder / GeoNetworking: forwarder) has to be selected from a (possible) multitude of ITS-Ss possessing the data, which should be delivered to another ITS-S (security: requester / GeoNetworking: data sink). To minimize channel load, multiple delivery of the data to its destination should to be avoided.

In position-based routing mainly two mechanisms exist to select a packet forwarder. These are sender based and receiver based selection. A popular approach for selection of the packet forwarder by its sender is called greedy forwarding (Sommer and Dressler, 2015). Thereby, the sender tries to maximize a specific metric, typically the covered distance, by selecting a particular forwarder. Moreover, different mechanisms using distributed receiver based forwarder selection, from the set of possible forwarders, have been studied (Sommer and Dressler, 2015; Füßler et al., 2003; Blum et al., 2003; Heissenbüttel et al., 2004; Füßler et al., 2004). An important concept is the so called contention-based forwarding (CBF) scheme (Füßler et al., 2003). It has been shown that CBF outperforms its greedy forwarding counterpart in many scenarios. An overview of this field is provided in (Sommer and Dressler, 2015).

2.2 Attacker Model

We assume a single, static and active attacker, e.g., using an RSU. Its location is unknown to the legitimate ITS-Ss. Moreover, the attacker does not possess valid cryptographic material to sign VANET messages.

3 PROBLEM STATEMENT

Two major issues are introduced by certificate chain distribution in VANETs as briefly outlined in Section 1. They are discussed in Sections 3.1 and 3.2.

3.1 Normal VANET Operation

We assume normal VANET operation without presence of an attacker in this section. Requesting an AAC leads to a peak in channel utilization, as every receiver using the AAC includes its certificate chain in its next CAM. AACs are shared between many cars, e.g., such from the same manufacturer. To limit the amount of AAC requests in general, long term buffering of such certificates is discussed in Section 4.1.

As outlined in Section 2, the AAC distribution problem shows some similarities to packet forwarding within position-based routing protocols. Thus, Sections 4.2 and 4.3 study possibilities to reuse concepts from GeoNetworking protocols. The key difference between forwarding and an AAC response is that for AAC requests the initial sender is identical to the (end-)receiver. In contrast, for forwarding the initial sender wants to deliver a packet to another ITS-S.

In general maximum message size within VANETs is strictly restricted, e.g., to 650 bytes in ETSI ITS (102, 2011). This is caused by the lack of message fragmentation support in current VANETs. Moreover, higher layer functionality does not know when the network layer security entity is about to include certificate(s) in a message inside its so called security envelope (103, 2015). Thus, always the maximum size of the security envelope has to be reserved, which significantly limits the size of higher level data sets. For example, 356 bytes (security envelope meta data + PSC + AAC (103, 2015)) have to be reserved for the security envelope within ETSI ITS, which is more than 50 % of the maximum message size. Limiting the amount of included certificates to one can limit the maximum size of the security envelope. Thus, an approach for such a limitation without introduction of extra authentication delay is developed in Section 4.4. It uses buffering of received but unverified PSCs and is shown to work well in combination with the responder selection approach from Section 4.2.

3.2 DOS Attack on AAC Distribution

To request emission of a stations certificate chain an unsecured explicit AAC request is used in current ETSI ITS and WAVE systems. This is similar to the unsecured explicit PSCs request scheme looked

at in (Bittl et al., 2015a) and standardized in (103, 2015). Thereby, the current design of the security system requires the usage of unsecured messages to trigger AAC and PSC distribution. The main reason for this is the legitimate possibility of two (or even more) ITS-Ss meeting without any prior knowledge of each others certificate chains, except of the commonly known root certificate(s).

In such a case there is no possibility for performing a secured request for the certificate chain of another ITS-S without sending the certificate chain of its own ITS-S. Thus, an attacker without access to legitimate cryptographic material can still misuse the AAC request mechanism to significantly increase channel load in the following way.

The attacker sends CAMs (or BSMs), which contain just a varying random value as the signer identifier and identifiers of valid AACs in the so called *request unknown certificates* header field of the security envelope. The signature can be filled by random values, too. Receivers cannot verify the attacker's messages, as they do not possess a PSC for the used signer identifier (with high probability). Thus, the invalid signature will go unnoticed. The attacker can obtain AAC identifiers for his requests from received CAMs of legitimate ITS-Ss in his surrounding due to cyclic inclusion of PSCs containing their corresponding AAC identifier (103, 2015). Up to six AACs can be requested in each CAM sent by the attacker.

In order to maximize the increase in channel load caused by the attack, the attacker selects the AACs used by the biggest share of ITS-S in its current surrounding. Thereby, he maximizes the number of ITS-Ss responding to his own CAMs by transmitting their certificate chain together with their next CAM. Using the maximum legitimate CAM generation rate (10 Hz (103, 2015)), the attacker can be assumed to be able to cause all successfully targeted ITS-Ss to include their certificate chain in each of their sent CAMs. Thereby, the channel load caused by these stations gets increased threefold.

In the worst case, all ITS-Ss in the attackers communication range only use six different AACs. Thus, he can target all these ITS-Ss. Hence, it can be expected that the channel load is increased by a factor of more than three. In case the wireless channel does not provide enough spare capacity to allow for transmission of the increased data volume, message sending by the ITS-Ss will be massivly delayed (by CSMA-CA waiting times). Moreover, the probability of collisions on the wireless channel is increased significantly. Thus, the attacker has performed a successful denial of service attack against ITS-Ss.

Furthermore, as the attacker does not provide a valid PSC in its CAMs but only a random hash value, he also causes all vehicles with in its communication range to always include their PSC within every single CAM. This attack on the unsecured implicit certificate request scheme is described in detail in (Bittl et al., 2015a). Thereby, it was shown that channel usage of all targeted stations can be more than doubled. Additionally, the area of effect of the attack is not limited to the broadcast area of the attacker. Instead, the increase in channel usage will only vanish at about two times the communication range of the attacker (Bittl et al., 2015a).

Section 5 provides an evaluation of the outlined attack alongside with the influence of efficiency increasing mechanisms proposed in the next section.

4 EFFICIENT AA CERTIFICATE DISTRIBUTION

To allow ITS-Ss to verify the authenticity of other ITS-Ss' PSCs AA certificates (AACs) are used. The impact of the distribution of such AACs on VANET system performance is outlined in Section 3 giving the general problem statement. Multiple approaches to overcome the outlined performance issues are discussed in Sections 4.1 to 4.4.

4.1 Long Term AA Certificate Buffering

In contrast to PSCs, the same AAC will be used by a multitude of ITS-Ss, e.g., by all vehicles from the same manufacturer running its own authorization authority. Moreover, the lifetime of AACs can be expected to be much longer than the one of PSCs, as there is no requirement for pseudonymity of AACs.

Thus, the exchange rate of AACs can be expected to be significantly limited by permanently buffering received AACs in the HSM (hardware security module containing the secure storage of cryptographic material) of an ITS-S after its verification by the help of stored root certificates. Otherwise, an ITS-S has to request all AACs anew each time it starts up. Thus, in areas with many vehicle upstarts, e.g., parking spaces, there will always be a high amount of AAC requests.

Current VANET standards do not specify how long a receiver should keep a received certificate. Clearly, there is a trade off between additional memory space requirements inside the HSM and the decrease in channel load by sparing AAC emissions. However, the overall number of AACs can be expected to be limited and the impact on channel load by AAC emission can be significant, at least for the currently standardized approach as shown in Section 5.2.

4.2 Requester Selection of Responder

One possibility to avoid multiple AAC deliveries after an AAC request is to let the requester especially choose an ITS-S who should respond to the request. In GeoNetworking forwarder selection by the sender is often realized via a greedy forwarding approach. Thus, we call such kind of requester selection of the responder to an AAC request *greedy responding*.

This approach can be simply implemented within the current ETSI ITS framework. The requester just adds the ID of the PSC (of the asked ITS-S) alongside with the ID of the AAC in the so called "request unrecognized certificates" header field of the security envelope. According to (103, 2015), this ID would be the so called HashedID3 of the corresponding certificate. It is determined by taking the lowest three bytes of the SHA-256 hash value of the certificate. This approach would mean that an ITS-S would only respond to an AAC request in case also its own PSC gets requested within the same request.

The impact of the DOS weakness from Section 3.2 is limited by a limited maximum length of the request list. E.g., at most six IDs are used within ETSI ITS. Thus, only the next messages of five ITS-Ss can be enlarged by the attack. Without presence of an attacker, only one ITS-S will respond to the request instead of a possible multitude of them.

However, effectiveness of requester based selection faces a major drawback. AAC requests typically occur when the environment of a vehicle is changing. Therefore, the requester may not be aware of all vehicles within its (new) communication area. Thus, responder selection may be sub-optimal as some available responder candidates for the selection process may be unknown to the requester or stations known to the requester left its communication range.

Possible selection mechanisms based on positions or sending times of known ITS-S in the requester's surrounding are discussed in the following sections. Clearly, such mechanisms are only required in case the set of possible responders to an AAC request has more than a single member.

4.2.1 Position based Selection

The requester chooses the AAC provider in a way to maximize probability for a successful bidirectional communication (request and response). Thereby, different strategies can be used, which are a

- simple strategy just using the position of possible responders, and
- advanced strategies using an environment model of the requester ITS-S.

Required data like position, speed and heading of ITS-Ss is contained in cyclically distributed messages (CAMs / BSMs). For the simple strategy, the requester minimizes the distance between both ITS-Ss. Thereby, it tries to maximize chances that the chosen ITS-S really receives the request and also its reply is successfully delivered to the requester. This strategy assumes that the probability of two ITS-Ss exchanging data successfully increases with decreasing distance between these ITS-Ss. This strategy is used in the evaluation provided in Section 5.2.

Advanced strategies could use a model describing the communication conditions within the requester ITS-S's environment. An approach to generate such a model, which is among other inputs based on digital maps, is described in (Boban, 2012). However, real time maintenance of such models is still a challenge due to high computational requirements.

Clearly, this approach does not guarantee to answer the request in minimal possible time. Time to delivery of the AAC ($t_{delivery}$) is determined by both CAM generation intervals at requester ($\Delta t_{CAM,requester}$) and responder ($\Delta t_{CAM,responder}$) due to the used piggybacking strategy for AAC distribution.

$$t_{delivery} \leq \Delta t_{CAM,requester} + \Delta t_{CAM,responder}$$

Thus, it can take up to two seconds until the AAC request gets answered. Due to high mobility of ITS-Ss in VANETs, it is quite likely that the responder is no longer the closest possible responder when it transmits the AAC to the requester. Therefore, this method has to be regarded as sub-optimal. However, it provides the benefit of simplicity. In order to reduce the chance of a long time span until AAC delivery, the following strategy uses the next expected sending time as the main criteria to select the responder.

A similar approach from packet forwarding is to try to cover the maximum possible distance towards the (final) receiver by each forwarding hop. Due to this maximization the approach is called a greedy one.

4.2.2 Sending Time based Selection

An AAC requester can try to minimize the time span Δt until the requested AAC is delivered. In systems using fixed message sending intervals, e.g., WAVE, the receiver can directly calculate the next sending time of all stations from whom he received messages based on the contained sending time stamps (within the security envelope). However, for CAMs in ETSI ITS message generation rate varies (302, 2014).

The current CAM generation interval of an ITS-S is determined from vehicle dynamics, e.g., speed or turn rate, which are themselves part of CAMs. Moreover, the current generation interval is contained in

every CAM. Assuming that vehicle dynamics are quite constant in the short time span between generation of two CAMs, the receiver of a CAM can determine a hypothesis about the next CAM sending time.

4.2.3 Position and Time based Selection

Advanced strategies could combine position and time information to improve AAC distribution in comparison to simple strategies like the ones proposed before.

An approach could use trajectory prediction to obtain an hypothesis about the future position of a possible responder at the point in time it is to send its next message. Afterwards, the position-based selection algorithms from Section 4.2.1 can be used with the position hypothesis as the input instead of the last received position. However, to obtain the parameters of the trajectory model, the requester has to analyze message content which could not be verified in advance, e.g., the speed of other ITS-S inside the CAM content. Thus, an attacker can try to send malicious messages to the message parser.

Another approach to combine time and position information is to use a weighting function. Thereby, each possible responder i is assigned a weight r_w, which characterizes its feasibility as a responder.

$$r_w = w_1 \cdot d_i + w_2 \cdot \Delta t_i$$

The individual weighting factors w_1 and w_2 can determined offline via simulation based evaluation of different scenarios leading to AAC requests. As both criteria d_i and Δt_i should be small to ensure successful rapid AAC delivery, low values of r_w show better responder feasibility than high ones. Thus, the ITS-S with lowest assigned value of r_w should be selected.

Adaptation the weights to current communication conditions is probability hard to realize, as AAC dissemination will not occur frequently in practice.

A more detailed analysis on advanced multi criteria based responder selection is subject to future work.

4.2.4 Attacking Requester Selection

An attacker can try to deny an ITS-S from obtaining an AAC by sending messages to the requester, which will always make him the target of the AAC request. For example, the attacker can claim to be very close to the requester. In case simple position-based responder selection is applied at the requester, the attacker will be the target of the request with high probability. After receiving the request, the attacker simply drops it. Thus, the ITS-S does not receive the AAC it wants to know about until it selects another responder.

However, to carry out the attack, the attacker needs to claim its availability as a possible responder in advance to the request. This means, that the attacker would need to know that a targeted ITS-S does not know about a certain AAC which it needs to know about. This is clearly an internal status of the ITS-S, which is not known to other ITS-Ss until the request has been transmitted. Thus, the feasibility of the outlined attack to be carried out in practice can be expected to be very low.

4.3 Decentralized Responder Selection

Decentralized receiver based selection of a forwarder in GeoNetworking, e.g., via contention-based forwarding (CBF), was shown to outperform the greedy forwarding approach (Füßler et al., 2004). In analogy to CBF we call our approach *contention-based responding (CBR)*. To request an AAC one just sends out the request, e.g., as in (103, 2015). However, the number of responses to the request is limited by decentralized coordination among possible responders.

After reception of an AAC request, all proper receivers start a timer. The AAC is only included after a timeout has happened. In case inclusion of the AAC by another ITS-S is detected before own AAC inclusion, the timer is canceled and the AAC is not included. Appropriate selection of the required timeout values is discussed in Sections 4.3.1 and 4.3.2.

This approach includes all possible responders into the responder selection process. Thus, the problem of incomplete knowledge about an ITS-S's environment, as outlined in Section 4.2 for the greedy approach, can be overcome.

4.3.1 Position and Timeout based Responding

The initial proposals of CBF in (Füßler et al., 2003; Füßler et al., 2004) suggest to use position and time based selection of forwarders. As initial sender and (final) target of the AAC request are identical, the selection criteria of CBF has to be changed to obtain a suitable CBR concept.

Thus, the timeout function of CBF (Füßler et al., 2004) is modified to obtain the CBR timeout function

$$t = \begin{cases} t_{CAM,i} \cdot \left(1 - \frac{d_i}{d_{max}}\right) & 0 \leq d_i < d_{max} \\ \infty & \text{otherwise} \end{cases}. \qquad (1)$$

Additionally, as in CBF an ITS-S which monitors that another ITS-S answered the request cancels its own timeout and thus does not include the AAC itself.

The intended effect of Equation 1 is illustrated in Figure 2.

Thereby, the most left vehicle has just sent out an AAC request. The time until the next message is to be sent by the individual vehicles $t_{CAM,i}$ is illustrated via the filled part of (right) cycles next to the vehicles.

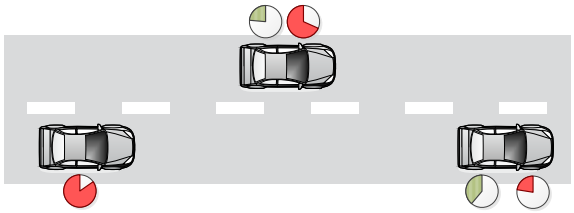

Figure 2: Response times under combined position and time CBR and pure timeout based responding.

The left cycle illustrates the effect of applying Equation 1 to calculate the timeout until responding with an AAC being included in the security envelope. The initial sender of the request has no such timeout.

One can see that the right vehicle is the first one to send a message after the AAC request, but it is not going to include the AAC into this message as the timeout will happen after sending the message.

As this approach minimizes the distance between requester and responder d_i, the set of vehicles receiving the response can be assumed to be similar to the set of vehicles which received the request. Thus, the amount of unnecessary extra responses caused by the hidden station problem should be low.

However, as many vehicles share the same AAC, it is pretty likely that the AAC requester will receive more than one CAM with the same AAC being part of their corresponding certificate chains. All these messages have to be discarded, as they cannot be validated. This is called cryptographic packet loss in (Feiri et al., 2012). The strategy proposed in the next Section 4.3.2 tries to minimize such packet loss at the cost of increased probability for duplicate responses.

4.3.2 Pure Timeout based Responding

A simpler variant for decentralized responder selection is given by using only a responding timeout and discarding the location information used in the above outlined approach from Section 4.3.1. The straight forward timeout period is given by the time until the next message is sent. Like in the concept proposed in the section before, an ITS-S cancels its timer when it receives a response from another station.

This concept minimizes the time span until the request is answered. Thus, probability of cryptographic packet loss by discarding CAMs from other ITS-Ss also using the requested AAC is minimized, too.

However, as the distance between requester and responder is discarded, the set of vehicles receiving the first response can differ significantly from the set of vehicles which received the request. Thus, the probability of duplicate replies is much higher for this strategy than for the one proposed in Section 4.3.1.

Moreover, the responder could leave the communication range of the requester before sending the response. In the worst case, all other responders still receive the response. Hence, they cancel their own responses. Thus, the requester does not receive any response. To avoid this scenario, a responder can keep track of its current average communication range and check whether the position of the requester is within this range before sending the response. Otherwise, it should not send the response. This improvement can be used for the strategy from Section 4.2.2, too.

The pure timeout based concept is also illustrated in Figure 2 (right timeout). In contrast to CBR the most right vehicle will send the requested AAC to the requester and the vehicle in the middle will suppress its own AAC transmission.

4.4 Pseudonym Certificate Buffering

According to (103, 2015), an ITS-S whose AAC was requested has to include its certificate chain, containing the AAC and the current PSC, in the security envelope of its next message. However, a request for an AAC can only happen in case the sender had already received the station's PSC using the requested AAC before (see also Figure 1).

In order to remove the need for a transmission of PSC_B alongside with its corresponding AAC_B, station A could store PSC_B in a buffer for later verification before requesting AAC_B. This means that station B just has to send a message (e.g., CAM) containing a single certificate shortening the message by more than 33% or about 133 bytes (103, 2015).

However, the mechanism is somehow more complicated when the scenario is extended to multiple communicating vehicles and multiple possible senders of the AAC. In this case, an ITS-S receiving a AAC request for its own used AAC cannot know whether itself caused this request or it was caused by another ITS-S using the same AAC. This can be changed by also applying the greedy requester selection algorithm from Section 4.2 before.

The combination of these two mechanisms is especially powerful. It enables to remove sending of certificate chains (containing PSC and AAC in a single message) completely from current standards. ITS-Ss only have to send either their PSC or their used AAC in the security envelope of CAMs, while there is no longer the requirement to send both of them at once. Thus, the worst case length of the security envelope can be reduced significantly by the size of a full certificate. The overall size of a message handed over the access layer is typically limited, e.g., in ETSI ITS to about 650 bytes (102, 2011). Thus, a shortened

worst case size of the security envelope leaves more message length to higher level protocols.

In contrast, in the CBR algorithm the AAC sender cannot know whether he caused the AAC request. Thus, combination of this approach is not possible with PSC buffering as it is outlined above. Therefore, the emission of a certificate chain, which contains PSC as well as AAC, is required for CBR for the responder to the request. Thus, CBR cannot limit the worst case size of a CAM security envelope as greedy responding together with PSC buffering can do.

Thus, there is a trade off between greedy responding and CBR. Thereby, CBR can be expected to provide the AAC with higher probability to the requester, as it can be assumed to be less susceptible to packet loss than its counterpart. However, greedy responding together with PSC buffering will yield less channel usage and a system design advantage. Hence, in detail evaluation of both strategies is required to show which one provides better VANET system performance.

To avoid a need for huge storage space for unauthorized certificates, one can remove them from the buffer after a timeout somewhat larger then the maximum sending interval of CAMs (which are used to distribute AAC). Additionally, the buffer can be maintained in a FIFO manner to limit its size to a well defined maximum. This kind of strategy is also proposed in (Bittl et al., 2015a) for PSCs and has been shown to perform well.

5 EVALUATION

In order to evaluate the impact of different AAC distribution mechanisms a simulation environment is used. Its details as well as the used traffic patterns are described in Section 5.1. Afterwards, the obtained results are discussed in Section 5.2.

5.1 Simulation Environment

The used simulation environment uses a combination of two dedicated simulators, which are SUMO for microscopic traffic simulation (Behrisch et al., 2011) and ns-3 for wireless network simulation (Riley and Henderson, 2010). Within ns-3 the ezCar2X framework is used to provide standard compatible ETSI ITS protocol functionality. An in detail description of the simulator can be found in (Roscher et al., 2014).

Furthermore, the simulations use the concept of so called core zones (102, 2012b; Kloiber et al., 2010). Thereby, the considered traffic area is a subset of the full simulated road network to avoid edge effects.

The used traffic scenario for all simulation is the well known freeway model. Thereby, three lanes are used for each direction, i.e., there are six lanes in total. Parametrization of traffic shape is done as suggested in (102, 2012b). Due to quite high vehicle speed, all ITS-Ss use 10 Hz CAM generation rate (302, 2014).

Channel simulation uses a two ray ground model with parameters from the freeway channel model derived by real measurements in (Cheng et al., 2007).

5.2 Evaluation Results

Evaluation results obtained by using the framework from Section 5.1 are given in the following. Thereby, the impact of the DOS attack from Section 3.2 is discussed first. Secondly, the impact on system performance without presence of an attacker is described.

5.2.1 DOS Attack

As mentioned in Section 3.2, the amount of requested AACs per CAM of the attacker is limited by the maximum length of the certificate request vector in the security envelope. Currently, the maximum length is six elements (103, 2015). Thus, in order to calculate the average amount of targetable vehicles in Germany we determine the market share of the six highest volume OEMs. This is done by using statistical data available from reference (Kraftfahrt-Bundesamt, 2014).

Thereby, we find that the accumulated market share of highest volume OEMs (VW, Mercedes, Audi, BMW, Opel, Ford) is 61.06%. Thus, on average an attacker can assume to successfully cause 61.06% of all vehicles within his communication range to significantly increase their channel usage.

The attack increases the average message size of CAMs by a factor of i over the ordinary CAM size (without presence of an attacker). Regarding cyclic inclusion of PSCs into CAMs an upper bound on the achievable increase can be calculated by

$$i \leq \frac{s_{\text{CAM,PSC+AAC}}}{\bar{s}_{\text{CAM}}}. \quad (2)$$

Thereby, the size of a CAM with certificate chain is given by $s_{\text{CAM,PSC+AAC}}$ (= 404 bytes) and the one of an average CAM by $\bar{s}_{\text{CAM}}$.

An upper bound on i can be obtained as follows. $\bar{s}_{\text{CAM}}$ is 108.5 bytes for 10 Hz CAM emission frequency and minimal 1 Hz PSC inclusion frequency. Thus, $i = 3.72$ is the upper bound on achievable increase in average message size. The bound is to be matched in case no implicit or explicit PSC requests happen in the VANET, which makes PSC inclusion happen more frequently. This increases average CAM size $\bar{s}_{\text{CAM}}$. Thus, i is smaller than the given bound. To

obtain the given values corresponding standards (103, 2015; 302, 2014) have been used.

The amount of PSC requests greatly depends on the traffic scenario, as such requests happen when the surrounding of ITS-Ss change. Thus, the achievable value of i depends on the traffic scenario, too.

The increase in average CAM size can be expected to cause an increase in channel load. Clearly, the channel load cannot supersede the maximum channel load determined by the maximum channel capacity. Thus, in case of an already high channel load the attack will cause the channel to saturate leading to significant system performance degradation. Thereby, mainly two effects can be seen, which are

1. reduced CAM generation rate on the facility layer enforced by decentralized congestion control (DCC), and
2. forced reduction of message emission frequency by denied channel access due to the used CSMA-CA mode on the access layer.

Both mechanisms reduce cooperative awareness among ITS-S by reduced update frequency of information about other ITS-Ss within their surrounding. Thus, data quality available for ADAS will decrease.

To simulate the attacker, we position an RSU in the center of our simulated area. It always sends out messages without PSC containing six AAC requests for the most commonly used AACs of ITS-S within its surrounding. Moreover, the attacker ignores DCC rules to send out his requests frequently even in case of already high channel load.

Table 1 gives achievable sizes of i within communication distance of the attacker. The vehicle interval for the displayed measurement results is three vehicles per second. This yields $\bar{s}_{\mathrm{CAM}} = 134.3$ bytes, due to an average of 3.064 PSC emissions per second. Additionally, for the first experiment all ITS-S were equipped with only six different AACs (column "worst"). For the second case, AACs were distributed according to OEM sales figures from (Kraftfahrt-Bundesamt, 2014). The attacker always requests the six most common AACs at once.

Table 1: Message size increase from DOS attack.

	worst	six most common AAC req.
bound	3.72	2.66
measured	3.01	2.23

The average communication distance in the used traffic scenario is about 300m. Thus, the increase in message size caused by the attack works up to a distance of 300m to the position of the attacker. Moreover, results from Table 1 show that the practically achievable increases are significantly lower than their corresponding bounds. This is caused by the fact that, in the reference scenario (without attacker) already a significant amount of PSC inclusions take place.

Channel busy ratio (CBR) is an important metric for channel load. Measured values for CBR in dependence on the distance from the attacker are given in Figure 3. Two displayed scenarios use the worst case in which all receivers include their certificate chain in their next transmitted CAM. Additionally, the corresponding scenarios, in which all ITS-Ss using the six most common AACs respond, are given. Vehicle density is varied by using two different intervals between vehicle insertion into the simulation (9s and 2s).

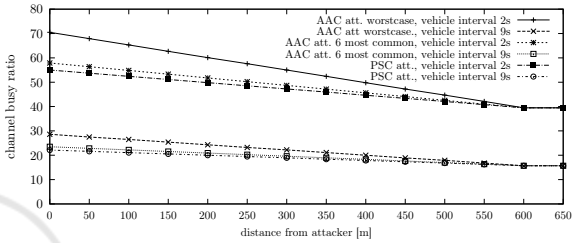

Figure 3: CBR in dependence of distance from attacker.

As a reference scenario, the pure attack on PSC distribution from (Bittl et al., 2015a), which is always part of the attack on AAC distribution as outlined in Section 3.2, is given in Figure 3. It serves as a lower bound for the channel busy ratio increase. CBR without an attacker is constant and equal to the one given for a distance of 650m to the attacker.

One can see from Figure 3 that the increase in channel load drops to zero at about 600m ($= 2 \cdot 300$m) distance to the attacker, i.e., double of the attacker's communication distance. The channel busy ratios for the DOS attack are higher than the ones for peak channel busy ratios on case of normal AAC requests (see Figure 4), due to the extra PSC distribution attack.

From comparison of the results from Table 1 and Figure 3, one can see that the channel load does not increase as much as the messages size does. This is due to saturation effects of the wireless channel, caused by the used CSMA-CA mechanism. Thus, ITS-Ss are (temporarily) denied from accessing the channel while the attack is present. Hence, the attacker can reduce frequency of message exchange and thereby decrease data quality (e.g., lower update rate) available for VANET applications.

Evaluation of countermeasures (AAC distribution according to Section 4) shows that they can all efficiently avoid the DOS attack. For all strategies, the increase in average message size and channel load is hardly noticeable even in case of frequently repeated AAC requests. The maximum observed amount of

responders for CBR was just two. For the other AAC delivery schemes only one node sent its AAC as expected. Thus, the massive amount of certificate chain emissions happening for the standardized approach can clearly be avoided by the proposed schemes.

The obtained results show clearly, that the DOS attack from Section 3.2 can be carried out and severely affects the usability of VANETs. Moreover, proposed strategies for more efficient AAC distribution can overcome this weakness.

5.2.2 Normal Traffic Scenario

In order to evaluate the impact on channel load we use two different metrics. The first one is the increase in average message size (see Equation 2) and the second one is the time span the increase persists.

The length of the period in which AAC responses from other ITS-S are sent depends on their current CAM generation rate. In case all ITS-S use a common generation rate of 10 Hz, the period should be about 100ms. Some transmissions will probably occur with a small extra delay, due to delays in internal processing within ITS-Ss and from channel access.

Four different cases have been studied in detail for AAC requests in respect to channel load. Thereby, the requester requests

1. one AAC and all other ITS-Ss answer the request (worst case),
2. the maximum of six different AACs being answered on average by 61.06 % of receivers,
3. one AAC which is equal to the most common on and thus the request is answered on average by 21.31 % of receiving ITS-Ss, and
4. one randomly picked AAC, which is answered on average by 8.6 % of receiving ITS-Ss (most right column in Table 2).

Thereby, the numbers were obtained from figures in (Kraftfahrt-Bundesamt, 2014).

Table 2 gives theoretical bounds as well as simulation results for both values at the location of the ITS-S sending the AAC request. The requesting ITS-S is inserted as an RSU into the simulation at its center after the remaining traffic flow has been already build up. Unfortunately, no reference scenarios have been suggested in prior work to simulate AAC requests.

Table 2: Message size increase after AAC request.

	worst	6 AAC	1 AAC	1 ACC a
bound	3.72	2.66	1.58	1.23
measured	3.01	2.23	1.43	1.17

The results in the first two columns of Table 2 are identical to those from Table 1. Requests for single AACs can be expected to be the most common case in practice. Corresponding values in Table 2 show that average message size increase is significant.

The average channel load, during the time responders send their certificate chains, is given in Figure 4.

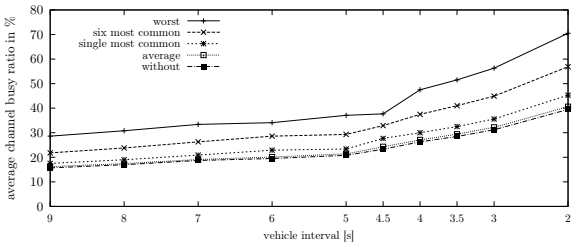

Figure 4: Channel busy ratios for different traffic densities after an AAC request at the position of the requester.

As can be expected, Figure 4 shows that the channel busy ratio increases alongside with increasing traffic density (i.e., decreasing vehicle interval). Additionally, an increase in the number of responders clearly increases the channel busy ratio. This shows that one can limit the channel busy ratio increase after an AAC request by limiting the number of responders, as done by the methods discussed in Sections 4.2 and 4.3.

The amount of channel busy ratio increase decreases with higher distances to the vehicle which sends the AAC request. Thereby, the distribution is like given in Figure 3. However, the increase last only for limited time, in contrast to the DOS scenario in Section 5.2.1 for which the increase is permanent.

Response times of the different efficient response mechanisms from Sections 4.2 and 4.3 are given in Figure 5. Moreover, performance of the standardized approach from (103, 2015) is illustrated. Both purely time based schemes limit responder selection to ITS-Ss within 300m distance to the requester.

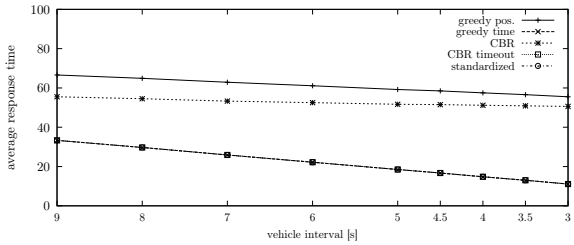

Figure 5: Response times for AAC requests (most common single AAC) for different traffic densities.

As one can see from Figure 5, the time based response mechanisms outperform their position based

counterparts. Furthermore, both schemes reach performance of the standardized approach. Moreover, the purely position based greedy responding schemes performs worst. The CBR scheme using time and position information cannot reach the performance of purely time based schemes. In detail analysis shows that many responses are delayed due to the location dependent timeout leading to a significant delay of an actually carried out AAC transmission. Furthermore, CAMs of the ITS-Ss which skipped transmitting the AAC are disregarded by the requester, as they cannot be verified due to the missing AAC.

In contrast to the position-based routing problem, no serious drawback of the requester based selection scheme in comparison to responder based selection was obtained. This is caused by the contrasting goals of cooperation between routing and AAC distribution. For AAC distribution the target of the caused reaction from the addressed responder(s) is the sender itself. In contrast, for packet forwarding the target is a distant node out of direct communication range of the sender. Moreover, forwarding can trigger message sending on its own, while AAC dissemination relies on piggybacking to higher level messages, e.g., CAMs.

Additionally, the time based response mechanisms yield minimal cryptographic packet loss. In the ideal case, no other ITS-S using the same AAC unknown to the requester transmits before the one distributing the AAC. Thus, the requester does not have to disregard further messages due to missing AACs.

Our evaluation shows that both proposed response time based AAC distribution schemes perform well. However, only the requester based selection scheme allows to avoid the transmission of entire certificate chains in one message completely. As this property can be very beneficial for the design of VANET protocols, the scheme from Section 4.2.2 should be used for AAC distribution in future VANETs.

6 CONCLUSIONS AND FUTURE WORK

Future VANETs require efficient security mechanisms to enable their usage in safety critical advanced driver assistance systems. We show that, apart from the distribution of pseudonym certificates, which has been well studied in prior work, also the distribution of authorization authority certificates (AACs) can significantly influence system performance.

The supplied analysis and evaluation of the current standard from ETSI ITS (103, 2015) shows that the straight forward approach taken there can lead to significant performance issues. Moreover, it allows an attacker to perform a serious denial of service (DOS) attack on VANETs, whose impact range exceeds the transmission distance of the attacker. Multiple approaches to minimize the number of required AAC emissions are discussed.

In general the frequency of AAC requests can be greatly limited by long term buffering of received AACs. Thereby, repeated distribution can be avoided. Additionally, requester or responder based responder selection schemes for AAC distribution can significantly reduce the number of AAC emissions after an AAC request. Thereby, the DOS attack can be avoided by design. Moreover, buffering of PSCs leading to an AAC request together with greedy responding completely removes the need for distribution of certificate chains. Thereby, the worst case size of the security envelope, and thus the security overhead, can be reduced by more then one third.

Thus, the proposed greedy response scheme, based on predicted message transmission time of possible responders, can be regarded as a promising approach for usage in future VANET systems.

Future work can study the influence of different traffic conditions on the performance of the suggested AAC distribution mechanisms. Thereby, the influence of variable rate CAM emission on prediction of response times at the requester can be studied in low and medium velocity traffic scenarios.

REFERENCES

(2011). Intelligent Transport Systems (ITS); Decentralized Congestion Control Mechanisms for Intelligent Transport Systems operating in the 5 GHz range; Access layer Part. V1.1.1.

(2011). Memorandum of Understanding for OEMs within the CAR 2 CAR Communication Consortium on Deployment Strategy for cooperative ITS in Europe. V 4.0102.

(2012a). Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management. V1.1.1.

(2012b). Intelligent Transport Systems (ITS); STDMA recommended parameters and settings for cooperative ITS; Access Layer Part. V1.1.1.

(2013). IEEE Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages. 1609.2-2013.

(2013). Intelligent Transport Systems (ITS); Security; Security header and certificate formats. V1.1.1.

(2014). Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service. V1.3.2.

(2015). Intelligent Transport Systems (ITS); Security; Security header and certificate formats. V1.2.1.

Behrisch, M., Bieker, L., Erdmann, J., and Krajzewicz, D. (2011). SUMO - Simulation of Urban MObility: An Overview. In *The Third International Conference on Advances in System Simulation*, pages 63–68.

Bittl, S., Aydinli, B., and Roscher, K. (2015a). Effective Certificate Distribution in ETSI ITS VANETs using Implicit and Explicit Requests. In M. Kassab et al., editor, *8th International Workshop Nets4Cars/Nets4Trains/Nets4Aircraft*, LNCS 9066, pages 72–83.

Bittl, S., Gonzalez, A. A., Spähn, M., and Heidrich, W. (2015b). Performance Comparison of Data Serialization Schemes for ETSI ITS Car-to-X Communication Systems. *International Journal On Advances in Telecommunications*, 8:48 – 58.

Blum, B., He, T., and Son, S. (2003). IGF: A State-Free Robust Communication Protocol for Wireless Sensor Networks. Technical Report CS-2003-11, Department of Computer Science, University of Virginia.

Boban, M. (2012). *Realistic and Efficient Channel Modeling for Vehicular Networks*. Phd thesis, Dept. of Electrical and Computer Engineering, Carnegie Mellon University.

Cheng, L., Henty, B. E., Stancil, D. D., Bai, F., and Mudalige, P. (2007). Mobile Vehicle-to-Vehicle Narrow-Band Channel Measurement and Characterization of the 5.9 GHz Dedicated Short Range Communication (DSRC) Frquency Band. *IEEE Journal on Selected Areas in Communications*, 25(8):1501–1516.

Feiri, M., Petit, J., and Kargl, F. (2012). Evaluation of Congestion-based Certificate Omission in VANETs. In *IEEE Vehicular Networking Conference*, pages 101 – 108.

Füßler, H., Hartenstein, H., Martin, M., Effelsberg, W., and Widmer, J. (2004). Contention-Based Forwarding for Street Scenarios. In *1st International Workshop in Intelligent Transportation*, pages 155–160.

Füßler, H., Widmer, J., Käsemann, M., Mauve, M., and Hartenstein, H. (2003). Contention-Based Forwarding for Mobile Ad Hoc Networks. *Elsevier's Ad Hoc Networks*, 1(4):351–369.

J. Harding et al. (2014). Vehicle-to-Vehicle Communications: Readiness of V2V Technology for Application. Technical Report DOT HS 812 014, Washington, DC: National Highway Traffic Safety Administration.

Heissenbüttel, M., Braun, T., Bernoulli, T., and Wälchli, M. (2004). BLR: Beacon-Less Routing Algorithm for Mobile Ad-Hoc Networks. *Elsevier's Computer Communications Journal (Special Issue)*, 27(11):1076–1086.

Kargl, F., Schoch, E., Wiedersheim, B., and Leinmüller, T. (2008). Secure and Efficient Beaconing for Vehicular Networks. In *Fifth ACM international workshop on VehiculAr Inter-NETworking*, pages 82–83.

Kloiber, B., Strang, T., de Ponte-Mueller, F., Rico Garcia, C., and Roeckl, M. (2010). An Approach for Performance Analysis of ETSI ITS-G5A MAC for Safety Applications. In *The 10th International Conference on Intelligent Transport Systems Telecommunications*.

Kraftfahrt-Bundesamt (2014). Neuzulassungen von Personenkraftwagen im August 2014 nach Marken und Modellreihen. online. available http://www.kba.de/DE/Statistik/Fahrzeuge/Neuzulassungen/MonatlicheNeuzulassungen/monatl_neuzulassungen_node.html.

Masdari, M. and Barbin, J. P. (2012). Distributed Certificate Management in Mobile Ad Hoc Networks. *International Journal of Applied Information Systems*, 1(1):33–40.

Morogan, M. S. and Muftic, S. (2003). Certificate Management in ad hoc Networks. In *Symposium on Applications and the Internet Workshops*, pages 337–341.

Riley, G. F. and Henderson, T. R. (2010). The ns-3 Network Simulator. In Wehrle, K., Günes, M., and Gross, J., editors, *Modeling and Tools for Network Simulation*, pages 15–34. Springer Berlin Heidelberg.

Roscher, K., Bittl, S., Gonzalez, A. A., Myrtus, M., and Jiru, J. (2014). ezCar2X: Rapid-Prototyping of Communication Technologies and Cooperative ITS Applications on Real Targets and Inside Simulation Environments. In *11th Wireless Communication and Information*, pages 51 – 62.

Sen, J., Chandra, M. G., Balamuradlidhar, P., and Harihara, S. G. (2007). A Scheme of Certificate Authority for Ad Hoc Networks. In *18th International Workshop on Database and Expert Systems Applications*, pages 615–619.

Sommer, C. and Dressler, F. (2015). *Vehiclular Networking*. Cambridge University Press.

Task Force PKI, WG Security C2C-CC (2012). C2C-CC PKI Memo. Technical Report 1.7, Car2Car Communication Consortium.