Pre-distribution of certificates for pseudonymous broadcast authentication in VANET

Michael Feiri*, Rolf Pielage†, Jonathan Petit§, Nicola Zannone†, Frank Kargl*‡
*Services, Cybersecurity and Safety, University of Twente, The Netherlands
†Department of Mathematics and Computer Science, Eindhoven University of Technology, The Netherlands
‡Institute of Distributed Systems, University of Ulm, Germany
§University College Cork, Ireland

***Abstract*—In the context of vehicular networks, certificate management is challenging because of the dynamic topology and privacy requirements. In this paper we propose a technique that combines certificate omission and certificate pre-distribution in order to reduce communication overhead and to minimize cryptographic packet loss. Simulation results show that this technique is useful to improve awareness quality during pseudonym changes.**

Keywords*—*Pre-distribution, certificates, omission, pseudonym change, security, VANET.

I. Introduction

Applications of vehicular communication are built upon local wireless broadcast messages. These messages are used to create cooperative awareness and to enable event notification and information dissemination among vehicles. Some applications can have influence on safety of life systems in vehicles and therefore need strong security. The leading standardization efforts in this domain specify digital signatures and dedicated public key infrastructures to provide authentication and integrity of all messages [1], [2].

Adding security through the pervasive use of digital signatures does have an impact on the usage of bandwidth and computational resources. The choice of a suitable digital signature scheme is the main option for minimizing these costs. The increase of bandwidth overhead, however, depends not only on the choice of a digital signature scheme but more importantly on the distribution method of certificates. A deficiency in optimizing bandwidth usage leads to an increase of packet collisions in the wireless channel, and thus, can cause degradation of service quality for all applications, including safety-of-life applications.

Typically, a sender is expected to bundle all relevant certificates of a trust chain with each signed message. This allows recipients to fully validate the message. However, this creates a significant bandwidth overhead. Alternatives are on-demand requests of missing certificates or omission schemes that determine a frequency of omitting certificates. These two approaches are not mutually exclusive; for instance, IEEE 1609.2 [2] and ETSI ITS [1] allow both techniques as well as their combination. A number of omissions schemes have been proposed, e.g. POoC [3], NbCO [4], and CbCO [5]. The fundamental trade-off, however, is the introduction of cryptographic packet loss in the form of unverifiable packets [5]. Omission schemes need to balance the intended decrease of network packet loss (NPL) as a result of fewer collisions in the communication channel against the unintended introduction of cryptographic packet loss (CPL).

We propose to combine omission schemes with pre-distribution as a technique to reduce CPL while maintaining the benefits of omissions schemes. Pre-distribution anticipates the need for certificates and disseminates them proactively. Needs for certificates arise through the arrival of new vehicles in a geographic region, or through a switch of cryptographic identities with the intention of breaking linkability of vehicle movements over extended periods of time. We consider two utility classes of pre-distribution techniques, geographic and temporal pre-distribution, as these are the dimensions that define the reasons for pre-distribution to be effective.

In the following section we present the related work. In Section III we discuss simulation results that demonstrate the benefits of the certificate pre-distribution technique. Finally, Section IV concludes the paper with directions for future work.

II. Related Work

Predictive pre-distribution of certificates, to the best of our knowledge, was not proposed as a technique for certificate management in Vehicular Ad hoc Networks (VANET). Certificate distribution itself, however, is a well known challenge for public key infrastructures. The classic solution of delivering certificates is to include them with the signed messages. This method is commonly known in the context of S/MIME [6], where the size of messages is not a critical attribute. The alternative PGP/MIME [7] solution uses key servers as repositories of key material and web-of-trust information, which substitutes the canonical chain-of-trust model of certificates.

Vehicular communication is much more sensitive to bandwidth consumption than email delivery on the Internet. Additionally, the chances of not having connectivity to third-party resources such as key servers is much higher. Even if availability of key servers could be assumed, the round-trip time would be expected to be much higher than local wireless communication. Therefore, the direct exchange of certificates through ad-hoc networking channels is preferred over remote infrastructure access for vehicular communication.

An area of intense research considers alternative trust and authentication methods that do not require the exchange of explicit certificates. Identity-based signatures have been

proposed for use in VANET [8] and could eliminate the need for certification. A shift to attribute-based anonymous authentication [9] could similarly eliminate the need for certificates. However, operational aspects such as the speed of cryptographic primitives make these schemes unsuitable for applications in pure vehicular ad-hoc networking [10]. Assistance through road side units (RSU) could mitigate some of these issues [11], [12], but the uncertain availability of such additional infrastructure precludes consideration of such proposals in current standardization efforts.

Implicit certificates, e.g. ECQV [13], allow the reconstruction of a certified public key from the public key of a certificate authority, a chosen identifier, and implicit certification data. This can save a considerable amount of bandwidth, but does not remove the need to exchange certification data. In this work we do not consider compression of certificate data or exploitation of network communication effects. This includes techniques such as Fountain or Erasure codes, which have been proposed in the area of certificate revocation list distribution in VANET [14]. We consider the question of such encoding techniques to be orthogonal to the question of sending certificate material.

A major concern about pre-distribution of certificates is the impact on privacy through the potential reduction of unlinkability. The use of strong cryptographic identifiers creates traceability that exceeds the intention of creating local short-term cooperative awareness among trusted entities. To avoid tracking of vehicles locations, which indirectly represents personally identifiable information of the driver, it is expected that vehicles will receive a set of pseudonymous identifiers that can be changed unpredictably to avoid linkability beyond a short period of time.

Pseudonym change strategies are still a matter of active research [15]. Uncertainties exist about the achievable privacy level in terms of attacker uncertainty, especially under consideration that a core service of vehicular communication is the exchange of precise location and trajectory information to create local short-term traceability. Multiple studies [16], [17], [18] have shown that linkability can be achieved even when changing the pseudonym for every message, simply due to the interpretation of position and trajectory information.

Proposals have been published to artificially create uncertainty for observers by introducing errors in the position information [19] or to establish mix zones with silent periods [20]. This, however, might create severe disruptions in service quality for applications that rely in precise data quality. Levèfre et al. [21] have shown in the context of intersection collision avoidance that pseudonym changes with silent periods can cause drastic degradation of service quality. It appears plausible that open announcements for locally synchronized pseudonym changes [22] might be a solution to avoid degradation of service quality. This could even include a period of RSU-assisted or group-based encrypted communication to preserve unlinkability [23], [24]. Yet, it is unclear if the volatility of VANET topologies allows groups to be sufficiently stable or if road-side units can realistically be assumed to be available pervasively enough.

In this paper we rely on the assumption that local short-term linkability is unavoidable, and is in fact a central goal of vehicular communication. As we limit our proposal to local one-hop dissemination and to very short-term temporal prediction, we expect to not create any significant loss of unlinkability.

Parameter	Value
Field size	2.5 km x 1 km
MAC	802.11p, 6 MBit/s
Fading	Rayleigh
Pathloss	Two-ray ground
Noise	Additive
Simulation runs	5
Transmit power	20 dBm
Beaconing frequency	10 Hz
Payload Size	50 Bytes
Number of nodes	300

TABLE I. SIMULATION PARAMETERS

Parameter	Value
PKAlgorithm	nistp256
ECC Key Type	compressed
Single Cert Size	140 Bytes
Signature Size	65 Bytes

TABLE II. CRYPTOGRAPHIC SETTINGS

III. EVALUATION

A. Simulation setup and assumptions

To perform the simulations we used the JiST/SWANS [25] software with extensions by Ulm University[1]. In addition to that, we have developed our own extensions to support pre-distribution of certificates. We generated a 2.5 km by 1 km map using VanetMobiSim [26] and we defined vehicles driving from two starting points towards a single intersection and moving away again in four directions. Using this setup we can simulate different stages of congestion.

In the simulation we only consider the transfer of beacon messages over one radio channel. Beacon messages, such as Basic Safety Messages [27] or Cooperative Awareness Messages [28], are not the only messages types expected in vehicular communication, but we assume that these messages dominate the load. We configured the 802.11p communication channel at 6 MBit/s with a fixed transmission power of 20 dBm. The basic parameters for our simulation are in line with previous works by Schoch et al. [4]. A summary of relevant parameters is given in Table I.

For the format of beacon messages we follow the Basic Safety Message (BSM) format as specified in SAE J2735 [27], delivered as a 45 bytes DER encoded payload in a IEEE 1609.2 data message [2]. Optional Part II attributes of the BSM format or optional parts of the 1609.2 message format are not considered. The security services specified in IEEE 1609.2 offer different options for the cryptographic additions to messages. We selected the compressed representation of nistp256 keys and signatures. Chains of certificates are not considered. A summary of the cryptographic additions to our simulated messages is described in Table II.

The total size of messages depends on the added cryptographic material. Adding a payload of 45 bytes for the BSM and 5 bytes for headers to the cryptographic material will result in messages of 115 bytes when omitting the certificate.

[1]Website: http://www.vanet.info

Parameter	Value
Certificate omission scheme	CbCO
Attachment strategy	Large packets & Omission gaps
Extra hops	1
Maximum of certificates	1
Percentage of certificates in omission gaps	50%
Temporal period	20 beacon cycles

TABLE III. PRE-DISTRIBUTION SETTINGS

For every extra certificate the message size increases by 140 bytes. The beaconing rate in the simulations is fixed at 10 Hz, as suggested by SAE J2735 [27]. The pseudonym change is simulated between the first 60 and 65 beacon cycles, as this is a time when the Awareness Quality (AQ) [29] is relatively stable.

AQ measures the percentage of known surrounding vehicles over the total number of vehicles that should be known based on location and communication range. The sample rate for the collection of AQ measurements is fixed at 1 beacon cycle period, which corresponds to 100 milliseconds in our scenario.

For pre-distribution we have selected settings as shown in Table III. Additional certificates that are pre-distributed can either be added to messages already carrying certificates, thus generating extra large packets, or can be added to messages that do not have a certificate as a result of the certificate omission scheme, thus disseminating certificates in the omission gaps. In our simulations a maximum of one extra certificate is added to messages, and we only do one-hop distribution.

B. Simulation results and discussion

As mentioned before, we analyze two utility classes for pre-distribution, namely geographic and temporal pre-distribution. Geographic pre-distribution disseminates neighbor certificates while temporal pre-distribution disseminates future pseudonyms for a specific period before the actual pseudonym change. Vehicles receiving certificates cannot make the distinction between neighbor certificates or future pseudonyms.

Figure 1 shows the AQ of the vehicles in our scenario with and without geographic pre-distribution applied. Geographic pre-distribution shows little improvement at this time, but several improvements are possible such as disseminating certificates over multiple hops or only distributing certificates of vehicles heading to a certain geographical region. Privacy implications of these improvements should be carefully studied. It is worth noting that geographic pre-distribution does not perform worse than the default dissemination of beacons.

Pre-distribution becomes more effective in the stage when vehicles change their pseudonyms. To show the effectiveness of pre-distribution, we first analyze the effects of pseudonym changes on AQ. Figure 2 shows the AQ over time with and without temporal pre-distribution applied. The first step is to simulate a pseudonym change for all vehicles between 60 and 65 beacon cycles, without using any pre-distribution. Our simulation uses the Congestion Based Certificate Omission scheme (CbCO) [5] to decrease the NPL and minimize CPL. The graph shows an increasing AQ in the first 14 beacon cycles up to a level where it stays relative constant. These first 14 beacon cycles do not have decent AQ levels yet as this can be considered the initial period in which vehicles receive

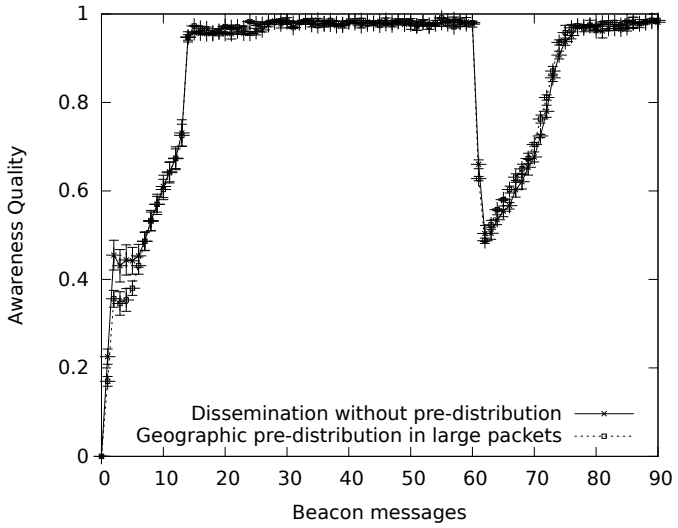

Fig. 1. Awareness quality without and with geographic pre-distribution (Large packets)

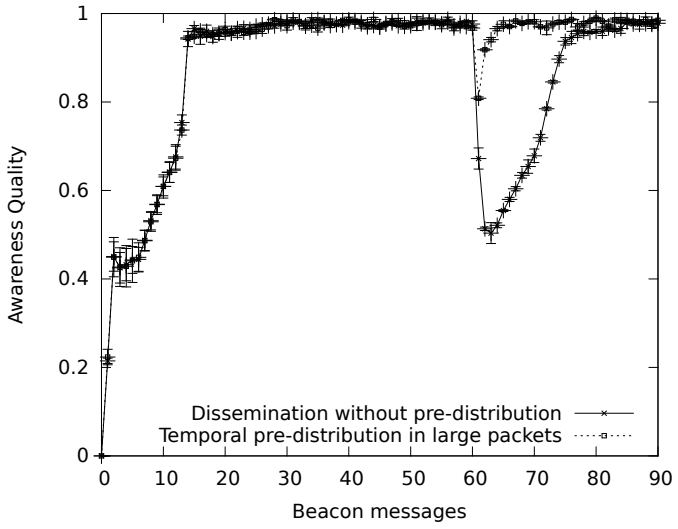

Fig. 2. Awareness quality without and with temporal pre-distribution (Large packets)

neighbor certificates, much like the first deployment of the V2V infrastructure. As this only happens at the deployment time, any negative effects in this period can be ignored as it does not affect safety.

In the period where the pseudonym change is performed for all vehicles, AQ drops significantly since all vehicles receive new identities which were previously not known to any neighbor. In order to increase AQ, these new identities need to be redistributed among as much neighbors as possible. Figure 2 shows that approximately 25 beacon cycles are needed to reach the previous AQ level.

The next step is to enable temporal pre-distribution, in which the future pseudonym is attached to existing certificates 20 beacon cycles before the pseudonym change. Thus, in the period from 20 beacon cycles before the pseudonym change up to the actual pseudonym change, certificates are attached

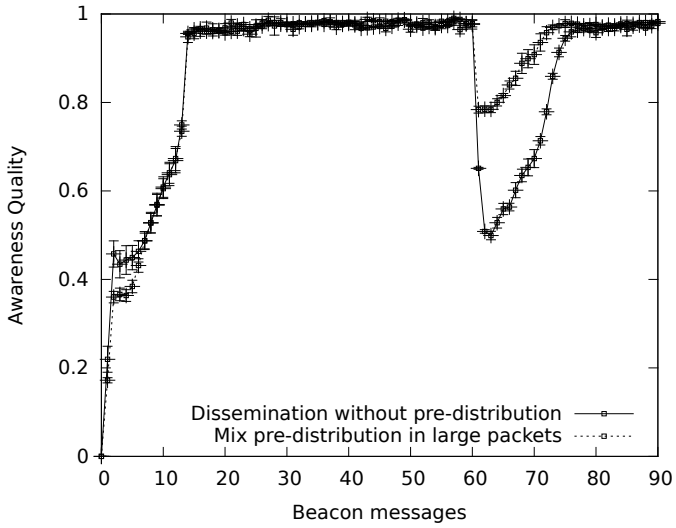

Fig. 3. Awareness quality without and with mix pre-distribution (Large packets)

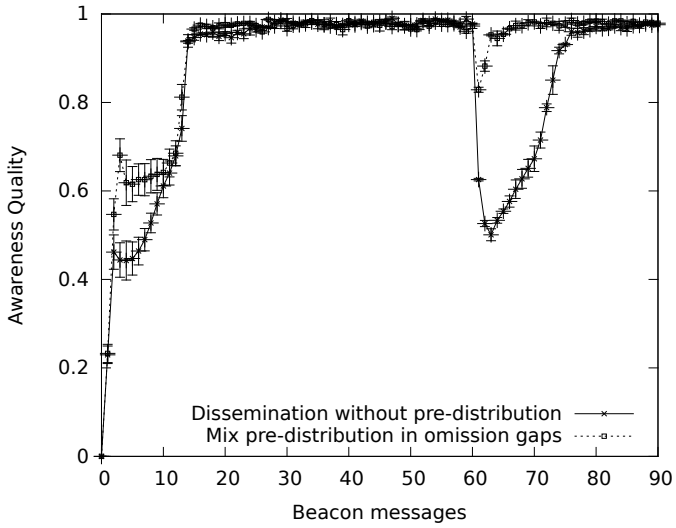

Fig. 4. Awareness quality without and with mix pre-distribution (Omission gaps)

based on the CbCO scheme. If this scheme requires attaching a certificate to the original message, the future pseudonym is attached as well. As shown in Figure 2, this technique results in a smaller drop of AQ at the point of the pseudonym change to about 50%. The AQ reaches the previous level in one or two beacon cycles, performing much better than the pseudonym change without pre-distribution.

As noted before, vehicles receiving certificates cannot make the distinction between neighbor certificates and future pseudonyms. Mixing these two techniques creates a higher level of privacy, although full privacy is not desired for local tracking.

Figure 3 shows the mix between geographical and temporal pre-distribution. Geographic pre-distribution is applied in the first beacon cycles up to 20 beacon cycles before the pseudonym change. At that point, either a future pseudonym or an existing neighbor certificate is pre-distributed randomly. After the pseudonym change, the scheme switches back to solely geographical. Due to the scheme more neighbors certificates and less pseudonyms are distributed. Therefore, the mix scheme reaches previous AQ levels slower than the temporal scheme, as shown in Figure 3.

For the simulations discussed above, we added certificates to messages already carrying a certificate, creating large packets. However, another option is to add certificates to messages without certificates, the so-called distribution in omission gaps. Distributing certificates in all omission gaps would not yield any effect as it neutralizes the effect of the omissions on the CPL. We have chosen to simulate the addition of certificates in omission gaps on a 50% basis. Further studies are required to investigate optimal strategies.

Figure 4 shows the AQ of vehicles with and without pre-distribution in omission gaps, while using the mix scheme for pre-distribution. The first period of the graph shows an improvement of AQ with pre-distribution. Distributing certificates in omission gaps results in a lower omission rate and, especially for the first period, this leads to significantly higher AQ. However, not taking into account the first period, we notice that the combination of omission gaps and mix scheme almost reaches the same result obtained with pure temporal distribution for large packets. The AQ drops to almost 80% and rises quickly to its previous level.

The use of the mix scheme, in which neighbor certificates and pseudonyms are combined, seems more efficient for the distribution of certificates in omission gaps. However, the main idea of using omissions is to reduce the amount of certificates sent. Sending certificates in omission gaps, however, increases the number of certificates that need to be sent, compared to sending large packets with extra certificates. Future research could indicate up to which level of congestion it is better to use omission gaps instead of large packets.

IV. Conclusion and Future Work

To ensure authenticated and pseudonymous V2X communication, certificates are appended to every location beacon sent. This generates a significant communication overhead, especially in terms of certificate management. To tackle this issue, we proposed a new technique that combines certificate omission and certificate pre-distribution. Simulation results demonstrated that pre-distribution of certificates does not eliminate cryptographic packet loss entirely. However, this technique can significantly reduce cryptographic packet loss caused by pseudonym changes while driving. Moreover, the introduction of certificate pre-distribution should be possible without requiring deep changes to existing architectures for certificate management in vehicular communication. As such we expect to see further practical evaluations of this technique to minimize service quality reductions due to the addition of security and privacy in vehicular communication.

As we limited the pre-distribution techniques to one-hop dissemination, the first future work is the evaluation of multi-hop dissemination. This will require more careful scoping rules to avoid wasteful usage of bandwidth, and a close investigation of privacy aspects. Indeed, wide-scale pre-distribution might

improve tracking capabilities of attackers that would otherwise have gaps and uncertainties in their coverage.

Another future work is the investigation of out-of-band channels, as in this paper, we exclusively considered certificate pre-distribution in-band within the same 802.11p communication channel. Alternative communication channels, possibly with different performance attributes, could be used to predictively maintain caches of certificates needed by vehicles.

ACKNOWLEDGMENTS

This work has been founded by the European Union's Seventh Framework Programme project PRESERVE under grant agreement no. 269994.

REFERENCES

[1] "Intelligent Transport Systems (ITS); Security; Security Services and Architecture," European Telecommunications Standards Institute, ETSI TC 102 731 V1.1.1, 2010.

[2] "IEEE Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages," IEEE Std. 1609.2-2013, April 2013.

[3] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy, "On the performance of secure vehicular communication systems," *IEEE Trans. Dependable Sec. Comput.*, vol. 8, no. 6, pp. 898–912, 2011.

[4] E. Schoch and F. Kargl, "On the efficiency of secure beaconing in vanets," in *Proceedings of 3rd Conference on Wireless Network Security*. ACM, 2010, pp. 111–116.

[5] M. P. Feiri, J. Y. Petit, and F. Kargl, "Evaluation of Congestion-based Certificate Omission in VANETs," in *Vehicular Networking Conference*. IEEE, 2012, pp. 101–108.

[6] B. Ramsdell, "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification," RFC 2633, 2004.

[7] M. Elkins, "MIME security with pretty good privacy (PGP)," RFC 2015, 1996.

[8] P. Kamat, A. Baliga, and W. Trappe, "An identity-based security framework for VANETs," in *Proceedings of 3rd International Workshop on Vehicular ad hoc networks*. ACM, 2006, pp. 94–95.

[9] J. Camenisch and E. van Herreweghen, "Design and implementation of the idemix anonymous credential system," in *Proceedings of 9th Conference on Computer and Communications Security*. ACM, 2002, pp. 21–30.

[10] P. Papadimitratos, A. Kung, J.-P. Hubaux, and F. Kargl, "Privacy and identity management for vehicular communication systems: a position paper," in *Proceedings of Workshop on Standards for Privacy in User-Centric Identity Management*, 2006.

[11] C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen, "An efficient identity-based batch verification scheme for vehicular sensor networks," in *Proceedings of 27th Conference on Computer Communications*. IEEE, 2008.

[12] H. Zhu, W. Pan, B. Liu, and H. Li, "A lightweight anonymous authentication scheme for VANET based on bilinear pairing," in *Proceedings of 4th International Conference on Intelligent Networking and Collaborative Systems*. IEEE, 2012, pp. 222–228.

[13] D. R. Brown, R. Gallant, and S. A. Vanstone, "Provably secure implicit certificate schemes," in *Financial Cryptography*. Springer, 2002, pp. 156–165.

[14] P. P. Papadimitratos, G. Mezzour, and J.-P. Hubaux, "Certificate revocation list distribution in vehicular communication systems," in *Proceedings of 5th International Workshop on VehiculAr Inter-NETworking*. ACM, 2008, pp. 86–87.

[15] J. Petit, F. Schaub, M. Feiri, and F. Kargl, "Pseudonym schemes in vehicular networks: A survey," *Communications Surveys Tutorials*, 2014.

[16] H. Stubing, A. Jaeger, C. Schmidt, and S. A. Huss, "Verifying mobility data under privacy considerations in Car-to-X communication," in *Proceedings of 17th ITS World Congress*, 2010.

[17] B. Wiedersheim, Z. Ma, F. Kargl, and P. Papadimitratos, "Privacy in inter-vehicular networks: Why simple pseudonym change is not enough," in *Proceedings of 7th International Conference Wireless On-demand Network Systems and Services*, 2010, pp. 176–183.

[18] N. Bismeyer, S. Mauthofer, K. Bayarou, and F. Kargl, "Assessment of node trustworthiness in VANETs using data plausibility checks with particle filters," in *Vehicular Networking Conference*. IEEE, 2012, pp. 78–85.

[19] B. Hoh and M. Gruteser, "Protecting location privacy through path confusion," in *Proceedings of 1st International Conference on Security and Privacy for Emerging Areas in Communications Networks*. IEEE, 2005, pp. 194–205.

[20] A. Beresford and F. Stajano, "Location privacy in pervasive computing," *Pervasive Computing*, vol. 2, no. 1, pp. 46–55, 2003.

[21] S. Lefèvre, J. Petit, R. Bajcsy, C. Laugier, and F. Kargl, "Impact of V2X privacy strategies on intersection collision avoidance systems," in *Vehicular Networking Conference*. IEEE, 2013, pp. 71–78.

[22] D. Eckhoff, C. Sommer, T. Gansen, R. German, and F. Dressler, "Strong and Affordable Location Privacy in VANETs: Identity Diffusion Using Time-Slots and Swapping," in *Vehicular Networking Conference*. IEEE, 2010, pp. 174–181.

[23] J. Freudiger, M. Raya, M. Félegyházi, P. Papadimitratos, and J.-P. Hubaux, "Mix-Zones for Location Privacy in Vehicular Networks," in *Proceedings of Workshop on Wireless Networking for Intelligent Transportation Systems*, 2007.

[24] A. Tomandl, H. Federrath, and F. Scheuer, "VANET privacy by "defending and attacking"," in *Proceedings of 6th Joint IFIP Wireless and Mobile Networking Conference*, 2013, pp. 1–7.

[25] R. Barr, Z. J. Haas, and R. van Renesse, "Scalable Wireless Ad hoc Network Simulation," in *Handbook on Theoretical and Algorithmic Aspects of Sensor, Ad Hoc Wireless, and Peer-to-Peer Networks*. CRC Press, Aug. 2005, ch. 19, pp. 297–311.

[26] J. Härri, F. Filali, C. Bonnet, and M. Fiore, "VanetMobiSim: generating realistic mobility patterns for VANETs," in *Proceedings of 3rd International Workshop on Vehicular ad hoc networks*. ACM, 2006, pp. 96–97.

[27] "DSRC Implementation Guide – A guide to users of SAE J2735 message sets over DSRC," SAE International, v20, February 2010. [Online]. Available: http://www.sae.org/standardsdev/dsrc/DSRCImplementationGuide.pdf

[28] "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service," European Telecommunications Standards Institute, ETSI EN 302 637-2, 2013.

[29] M. Feiri, J. Petit, R. Schmidt, and F. Kargl, "The impact of security on cooperative awareness in VANET," in *Vehicular Networking Conference*. IEEE, 2013, pp. 127–134.