Vehicular Communications 6 (2016) 1–6

Contents lists available at ScienceDirect

Vehicular Communications

www.elsevier.com/locate/vehcom

Distributed cross layer duplicate address handling for safety critical VANET communication

Sebastian Bittl

HU Berlin, Berlin, Germany

ARTICLE INFO

Article history:
Received 9 April 2016
Received in revised form 31 October 2016
Accepted 8 November 2016
Available online 14 November 2016

Keywords:
Duplicate address detection
Duplicate address resolution
VANET

ABSTRACT

Vehicular ad-hoc networks are in the wake of mass deployment within upcoming years. This dedicated kind of mobile ad-hoc networks in the automotive domain is of high interest to increase safety of driving. We find that prior approaches for duplicate address detection in such networks fail to cover significant use cases. Low available bandwidth and limited communication radius together with high node mobility lead to reduced presence of meta data, like routing tables. This, holds especially for non IP-based safety critical message exchange using dedicated VANET protocols. However, common address duplicate handing mechanisms rely on such meta data. We show that this can lead to failure of duplicate address detection for ETSI ITS and WAVE in safety critical use cases. This is caused by a variant of the well known hidden station problem. To overcome this weakness, we propose a cross layer aware duplicate address detection scheme in combination with active address change requests to resolve the duplicates. An evaluation within a simulation environment shows the feasibility of the approach.

1. Introduction

Mobile ad-hoc networks (MANETs) are an important topic in both research and practice. Vehicular ad-hoc networks (VANETs) are an important subset of MANETs, whose mass roll out is predicted within upcoming years. VANET standardization is mainly performed within US wireless access in vehicular environments (WAVE) and European ETSI intelligent transport systems (ITS) frameworks [1–3]. A rigid security system is required for VANETs, due to wireless data exchange and safety critical use cases.

Safety critical communication within a VANET is typically stateless, i.e., each message should be usable on its own. Dedicated communication protocols have been developed for this kind of data exchange. Their requirements arise from robustness against package loss, highly mobile participants and tough realtime requirements of use cases. Thus, each message is digitally signed to ensure authenticity and integrity. Required cryptographic parameters are contained in a security envelope, which embeds the message's payload at the network layer level. It holds per message parameters (e.g., the signature) and per node parameters (e.g., the public key), which are packed into certificates. These certificates are only sporadically piggybacked on messages to reduce average message size [4,5].

Duplicate address detection (DAD) is a well known problem in communication protocols. It arises from independent (i.e., uncoordinated) selection of addresses at individual nodes, as used within VANETs. Countermeasures typically rely on meta data like routing tables, which are not present in many VANET specific protocol stacks, e.g., in the WAVE system without support for multi-hop communication [1,6]. We find that this leads to a variant of the well known hidden station problem, which occurs on various protocol layers. VANET protocol stacks use node identifiers (i.e., addresses) on many protocol layers. Thus, DAD has to be performed on all these layers, too. However, this is not done by current standards. Only the ETSI ITS network layer uses DAD so far, but the applied mechanism only covers the case in which the own node is causing the duplication. A detailed problem definition is given in Section 2.

The need for DAD in regard to certificate IDs is specific to VANETs. Low communication bandwidth and high numbers of highly mobile nodes require frequent on the fly certificate distribution among nodes. This is done by piggybacking certificates on beacon messages. A-priori certificate distribution is infeasible, due to high numbers of nodes and frequent certificate changes by each node caused by privacy requirements [3,7]. To limit channel load, most messages do not carry their signer's certificate, but only an ID of it [4,5]. Such an ID is typically determined by using a hash function on the certificate. To further limit message size, IDs are limited in length, e.g., to eight bytes for WAVE and ETSI ITS. This

E-mail address: sebastian.bittl@mytum.de.

http://dx.doi.org/10.1016/j.vehcom.2016.11.002
2214-2096/

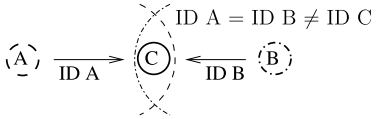

Fig. 1. Hidden station problem applied to duplicated addresses. Node C receives messages from A and B sharing an address. A and C cannot learn directly of each others presence.

leads to the risk of duplicate certificate IDs within communication range of a node, especially in scenarios with high node density.

The further outline is as follows. Section 2 gives a detailed problem statement. A review of related work is provided in Section 3. Section 4 describes the impact of duplicate addresses on functionality of various protocol layers of VANETs together with mechanisms to detect such duplicates. A decentralized scheme for fast DAD and duplicate resolution requiring only low overhead is proposed in Section 5. Moreover, an evaluation of the introduced mechanism is provided. Finally, Section 6 gives a conclusion about achieved results and possible subjects of future work.

2. Problem statement

Typically, DAD is performed by comparing a protocol address from a received message to the corresponding address of the receiver's node [8,6,3]. In case a duplicate is found, a duplicate resolution algorithm is applied. We call this internal DAD. Its detection is straight forward and resolution is often done by picking a random new address by the detector. This mechanism is typically applied in point to point communication networks.

An additional impact of address duplications occurs in VANETs using broadcast mechanisms for information distribution. Within such networks nodes suffer from the hidden station problem and missing or incomplete knowledge about the full network at each node. Thus, nodes may not become aware of address duplicates being caused by themselves. However, receivers of messages from multiple other nodes using duplicated addresses may suffer from them. Thus, receivers should detect such duplicates in a process we call external DAD. A scenario featuring a hidden station problem together with an address duplication is illustrated in Fig. 1.

The need for ensuring uniqueness of identifiers used in VANET communication protocols is mentioned in [7], but no methods to ensure this property are given. Moreover, internal DAD is standardized for the ETSI ITS network layer [8] and [9] calls for the same mechanism to be applied for the facility layer node identifier. To the best of the knowledge of the author, DAD has not been considered for remaining protocol layers. Moreover, the need for external DAD in VANETs has not been identified so far. Thus, it has not been treated in prior work.

To perform external DAD, a node checks addresses in a received message for equality to such addresses in prior messages. In contrast to internal DAD, the detector node cannot directly resolve the duplication on its own. Thus, it has to request such resolution from at least one node causing the duplication. Such kind of address change requests have not been proposed for the VANET domain so far.

We study the impact of external address duplicates on VANETs at the example of current ETSI ITS and WAVE approaches in Section 4. Cross layer efficient external DAD and duplicate address resolution are discussed in Section 5.

3. Related work

Research for decentralized DAD in MANETs has so far mainly concentrated on IP based networks [10,11,6,3] or other protocols with active network topology discovery at the network layer [12].

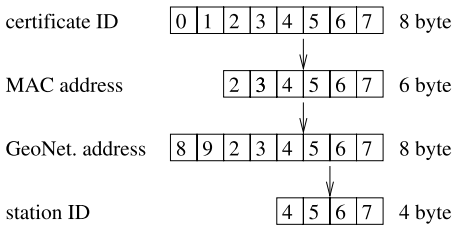

Fig. 2. Example for derivation of different addresses on various layers from a common station pseudonym (i.e., certificate ID).

However, many VANET protocols for safety critical ad-hoc communication are not IP-based. Thus, no meta data exchange for network topology discovery is performed [8,13,1,3]. Moreover, the so called passive DAD scheme from [6] does not fully work in a passive manner. Instead, it relies on active meta data (e.g., routing information) exchange caused by other functionality. It just re-uses this information instead of transmitting own data sets like done by other approaches, which are typically called active DAD schemes [14,6].

In the only fully passive approach for DAD, a receiver compares addresses of received packets with its own address, like in [8]. Within ETSI ITS this approach is used on the network layer. In case of a detected duplicated address, the detector changes its network layer ID as soon as possible. An extension of this scheme to the facility layer node ID is proposed in [9].

A proposal to avoid duplicated certificates in VANETs by coordinated checks of certificate authorities is discussed in [15]. However, this approach cannot avoid the certificate ID (or address) duplication problem, as differing certificates may have the same ID. Thus, the approach would need an extension towards also checking all addresses derived from all certificates. High numbers of certificate generations would lead to massive effort for performing all cross checks. This would further increase the already high effort required for running certificate authorities [1]. Thus, such kind of approaches are not considered in the following.

Within VANETs addresses on various protocol layers are typically coupled. This is caused by the need to bind the lifetime of other layers' addresses to the one of the current pseudonym (i.e., its certificate ID) to avoid node tracking [7].

An example for address (or ID) coupling is given in Fig. 2, with ETSI ITS nomenclature (WAVE is very similar). The procedure to derive individual addresses from a pseudonym has not been defined in standards so far. However, no need to use another approach than shortening has been found so far. Due to coupling of addresses, changing of any single address can be performed by performing a pseudonym change (with high probability).

4. Impact and detection of address duplication

The risk of an address collision increases alongside with smaller address ranges and increasing number of nodes. We use the WAVE/ETSI ITS protocol architectures to discuss the impact of duplicated addresses within received messages on various protocol layers. Possibilities to detect external duplicates are looked at, too.

4.1. Certificate ID

For certificate ID duplications, two cases need to be distinguished. In the first one, a message containing only a signer's certificate ID is received and the correct sender's certificate is not known to the receiver. Thus, the receiver looks up stored certificate(s) corresponding to the received certificate ID, to obtain cryptographic parameters required for message verification. This look-up succeeds, due to the ID's duplication. However, message

verification will fail, as the wrong certificate holding a non-fitting public key got used. Thus, the message is discarded. This issue is another source of so called cryptographic packet loss [16], which has not been found in prior work. The receiver cannot determine whether the message got manipulated by an attack or there is a duplicated certificate ID.

Moreover, after discarding the message its receiver needs to decide on how to proceed in regard to the certificate distribution mechanism. A pessimistic receiver assuming an attack simply discards the message. In contrast, an optimistic receiver assumes just a collision in the certificate ID field. Thus, he proceeds like after detection of a new neighbor, i.e., including his own certificate in the next beacon message and requesting the missing certificate. Thereby, the time to receiving the required certificate is minimized. Thus, we recommend to use this optimistic approach.

An attacker does not gain any advantage from usage of the optimistic approach. He can misuse it to cause emission of the certificate of the receiver, but this can be achieved anyway. It is just necessary to send a message with any new node ID to trigger the detection of a new neighbor, as outlined in [17]. Thus, capabilities of an attacker are not extended by the proposed approach. After the formerly unknown certificate got received, one proceeds as explained in the following.

Second case is reception of a message with a full certificate. Details of message handling are implementation specific. Typically, a sequence like the following is used. At first, the certificate ID is determined. The ID is used to check whether the certificate is already known and validated. This will succeed, due to the duplicated address. Then, the receiver proceeds as in the first case, i.e., verification will fail.

After the failed verification, the receiver should perform a more detailed comparison of the received certificate and the already stored one, e.g., byte per byte. Thereby, these will be found to be different with very high probability. Thus, the certificate ID duplicate can be detected. Then, the new certificate can be validated and used. Thus, the message containing the certificate causing a certificate ID duplication is not discarded by the verification procedure.

Without the described fallback mechanism after failed message verification, messages from the node causing the ID duplication will always be discarded even in case they carry a valid signing certificate and signature. Thus, the receiver will never achieve awareness about the sender, which clearly limits capabilities of applications relying on that data.

These findings show, that the security entity can handle the presence of certificate ID duplicates. However, other layers addresses are derived from certificate IDs and such layers cannot handle them well as explained in the following sections.

4.2. Medium Access Control (MAC) layer address

Many VANET specific MAC layer approaches, e.g., 802.11p and ITS-G5, only use MAC layer ACKs in unicast mode, but not in broadcast mode [18]. Thus, a duplicate MAC address will not interfere with broadcast communication. In unicast mode, it leads to acceptance and confirmation of messages by nodes which were not intentionally addressed by their sender. Thus, the sender will incorrectly assume that his message was received.

There should not be a significant impact on security of communication in VANETs by spurious superficial ACKs. However, there may be an impact on safety aspects due to reduced confidence of correct reception of a sent message.

The MAC address is often used as part of the network layer address in protocol stacks [6,8]. Thus, a duplicate MAC address will lead to a duplicate network layer address as well with high probably. For example, in ETSI ITS the network layer address is composed of the MAC address and remaining fields are filled according to static node properties, which are identical for many nodes [8] (see also Section 4.3).

The MAC layer has no option to detect externally duplicated addresses without parsing higher layer content, which is discouraged to maintain clear separation of layers.

4.3. Network layer address

Network layer addresses are typically used for packet routing. VANETs without support for multi-hop communication, e.g., WAVE, make only very limited use of this address [3]. ETSI ITS uses it for duplicate packet detection (DPD) together with a sequence number and sending time stamp [8].

To discard outdated/duplicated packets, the highest message sequence number and last sending time stamp is stored for each known communication partner. For each received message it is checked whether the sending time stamp is higher than the stored value. In case a smaller value is found the packet is discarded. Thus, in case of an externally duplicated network layer address, the message from the node using a lower time stamp value is discarded. In case of an equal sending time stamp, the message from the node using a lower sequence number is discarded. For more details see [8].

This discarding of messages leads to another source of packet loss, which has not been identified in VANETs so far. In case of ETSI ITS, the network layer's so called GeoNetworking address is significantly longer than the MAC address. However, the part enlarging the contained MAC address is identical for most stations, as it is derived from static station properties (fields labeled 8 and 9 in Fig. 2). Thus, the collision probability for a GeoNetworking address is almost the same as for a MAC address.

The network layer cannot distinguish repeated/outdated packets form those with externally duplicated addresses. Moreover, ETSI ITS applies internal DAD by checking for equality of both the network and MAC layer addresses. This avoids incorrect DAD for multi-hop broadcast communication during which the sender may receive its own packet from a forwarding node. However, this also limits applied DAD to a single-hop neighborhood.

4.4. Station address

Within VANET applications each node is typically assigned an ID (i.e., address), which is part of the individual application's message type. For example, beacons within ETSI ITS and WAVE use a station ID to enable local tracking of vehicles [3]. It is considered a unique ID. No duplicate detection or resolution mechanisms for it have been suggested so for WAVE. Internal DAD for the ETSI ITS facility layer station ID is proposed in [9].

VANET applications require to distinguish other nodes, e.g., to enable object tracking for collision avoidance. It can be assumed that such kind of algorithms will be confused by duplicated node IDs. For example, some messages could be discarded as being implausible as they would require unrealistic object movement. In doing so, dangerous situations may go unnoticed or incorrect warnings (i.e., false positives) could be issued. This is especially critical for the planned safety critical use cases of VANETs.

5. Duplicate address handling

To realize reliable DAD in a VANET with coupled addresses on different layers (like illustrated in Fig. 2) a cross layer detection mechanism is proposed in Section 5.1. Once an address duplicate gets detected, the algorithm from Section 5.2 can be used to resolve it. Feasibility of the proposed mechanisms within VANETs is shown in Section 5.3.

5.1. Cross layer duplicate address detection

As outlined in Section 4, many protocol layers cannot detect external address duplications in general. However, the security entity can do this with high probability. Fortunately, it treats messages before these are handed over to the main network layer mechanisms and further higher layers (WAVE or ETSI ITS protocol stack). Thus, the security entity should perform DAD based on the received certificates and their certificate IDs. Such DAD includes to check for duplicates of the well known higher level addresses derived from a certificate ID.

Applications using non-standardized message exchange with custom node identifiers have to take care for possible duplicates themselves. However, deriving the custom ID from one of the standardized ones without shortening should be save.

Due to the given protocol architecture, collisions in the MAC address can only be detected after the MAC layer already handled the packet. Thus, sending of an incorrect MAC layer ACK, as described in Section 4.2, cannot be avoided by the given approach. To do so, one would have to delay sending of such ACKs until DAD has been done by higher layers. However, this is probably hard to realize due to tight timing conditions for sending MAC layer ACKs.

5.2. Duplicate address resolution

Mainly two approaches for cross layer duplicate address resolution over multiple layers can be thought of. Either one can try to keep the amount of changed addresses by a station as low as possible, e.g., only changing the network layer address, or one always changes all identifiers. The latter one is already done by the pseudonym change mechanism in current VANETs. Thus, we recommended this approach as it uses already existing mechanisms.

Individual address changes on dedicated layers break the typically fixed relation between addresses on different layers. For example, in ETSI ITS the network layer needs to determine the GeoNetworking address of a unicast target from its station ID, as the facility layer triggering message sending only provides the target's station ID. A similar dependency exists within the security entity. It has to map GeoNetworking addresses of target nodes to their certificates to enable message encryption. Thus, changing the address on one layer would cause a complicated set of updates on other layers. Such extra and close coupling of layers should be avoided.

To resolve an address duplicate, at least one node has to perform a pseudonym change. Thus, duplicate address resolution creates the need for an extra source of pseudonym changes, which is not related to privacy protection. Within ETSI ITS the security entity already provides an interface to request a pseudonym change [19]. However, its usage has not been defined in detail so far.

To resolve a duplicated address after internal DAD, the detector can just trigger a pseudonym change of itself. However, after external DAD found an address duplication, the detector needs to trigger another node to do so. No such mechanism has been considered yet. It can be realized by adding another on demand included header field to the security envelope. It holds a dedicated header field ID and the certificate ID of the node being requested to change its pseudonym. Such a header field would require nine bytes for ETSI ITS and WAVE. Thus extra content is small in comparison to a 93 byte minimum envelope size [4].

Moreover, the header field is only included on demand. Thus, the minimum size of the security envelope is not increased by the approach. For details about the importance of keeping this minimum size as small as possible see [16].

We prefer request piggybacking on beacons over dedicated request messages. In doing so, overhead and complexity caused by an extra message type can be avoided.

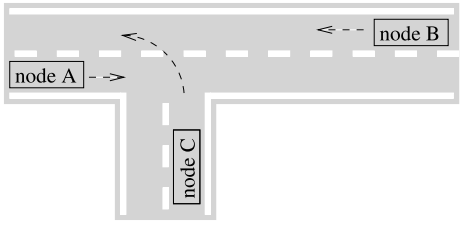

Fig. 3. Road layout representing a T-crossing.

In case a receiver finds its own certificate ID within the proposed extra header field, it changes its pseudonym immediately. To avoid misuse of this feature, the request is only to be accepted in case verification of the requester's message succeeded. This means, pseudonym change requests from nodes whose certificate (chain) is unknown are dropped.

Pseudonym changes lead to significant overhead on various layers [16]. Thus, their amount is to be minimized. Hence, a detector of an external address duplication tries to request only a single pseudonym change. However, in case of a certificate ID duplicate this is not possible using the above described mechanism. One would have to include the whole certificate or define an extended certificate ID with even lower duplication probably to do this. However, this is not recommended as this would significantly increase the worst case size of the security envelope, which should clearly be avoided as outlined in [16].

5.3. Evaluation

To evaluate the approaches described in Sections 5.1 and 5.2, they were implemented within the ezCar2X framework's simulation environment resembling an ETSI ITS based VANET [20]. This framework combines the traffic flow simulator SUMO (Simulation for Urban MObility) [21], the network simulator ns-3 [22,23] and the ETSI ITS compatible protocol stack from ezCar2X [20]. SUMO and ns-3 are coupled via the so-called TraCI (Traffic Control Interface) interface to obtain a common discrete event simulation environment. Node movement is simulated by SUMO, while communication on the physical and MAC layer is simulated by ns-3, with some ETSI ITS specific extensions to realize distributed congestion control (DCC). A pathloss model with Nakagami fading is used with parameters taken from [24]. The ETSI ITS protocol stack is installed on each node inside ns-3 individually.

Each tested traffic scenario was run with the original ETSI ITS protocol stack without the proposed duplicate address detection mechanisms, and also with an improved version of the protocol stack implementing the methods from Sections 5.1 and 5.2. Dedicated vehicles with intentionally set identical addresses on different layers were inserted into simulations.

The first used traffic scenario is illustrated in Fig. 3. A T-crossing is used as the road network's basic layout.

This first traffic scenario resembles a use case for an intersection collision risk warning. Node C wants to join a road on which nodes A and B travel. Node C needs to wait before entering the crossing until both nodes have passed by to avoid a collision with one of them. As a first step, the scenario was run with differing identifiers used by each node to ensure that the assistance system works well. Details about the implementation of the intersection collision risk warning application can be found in [25].

Moreover, a second traffic scenario resembling an overtake scenario on a rural road is considered. It is illustrated in Fig. 4.

The second traffic scenario resembles a use case for an overtake collision risk warning (or overtake assistant). Node C wants to overtake node A, which travels just before it on the same lane. Node B is approaching in the opposite direction on the second

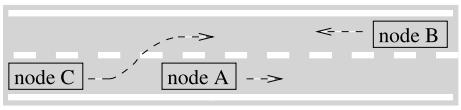

Fig. 4. Road layout representing a rural road.

lane. Node C has to delay its overtake maneuverer until node B has passed by to avoid a collision. As for the first scenario, a test run with differing identifiers for all nodes was performed to check the correctness of the collision avoidance application. It was implemented using the data processing mechanisms described in [25].

To test the impact of duplicated addresses on various protocol layers, these were set to identical values at nodes A and B when these nodes are inserted in the simulation. This procedure was tested for each layer's identifier. In doing so, dependent identifiers (see Fig. 2) were set accordingly.

The obtained results show that the described packet discarding (see Section 4) happens for the standardized approach. No cooperative awareness about either node A or B, whichever communicates later with node C, is achieved at the application layer of node C, in case any duplicated address is present. The identical station type of nodes A and B leads also to a network layer ID duplication, in case a MAC address duplication is present. Only in case of a pure station ID duplication, messages from the node (A or B), which comes into communication range of node C secondly, reach the application layer of node C. Otherwise, they are discarded at the network layer, either by the network layer itself or by the security entity. Even in case messages reach the application, it cannot differentiate both senders. Thus, it discards messages, as they are identified as implausible updates based on prior received information. Hence, the application can only avoid collision with one of the two possible collision partners.

In the first scenario (T-crossing), the presence of either node A or node B was not detected by the facility layer of node C during the conducted simulations. In the second scenario (rural road), node B was never detected at the facility layer of node C, as the communication between nodes A and C starts significantly earlier than between nodes B and C. This is caused by the fact that node C approaches node A earlier than approaching node B. Hence, the prior detection of node A blocks the detection of node B at node C.

The scheme proposed above (see Sections 5.1 and 5.2) is found to be able to detect and resolve the address duplications. Only the packets leading to initial detection of the duplication were lost. Successive packets after emission of the targeted address change request held different addresses. Thus, they were accepted by node C. Thus, node C was able to obtain awareness of both possible collision partners in time. Hence, the assistance system behaved like in the case without a present address duplication and collisions were successfully avoided.

6. Conclusions and future work

VANETs are a promising technology for increasing future safety of driving. Prior work has not studied duplicate address detection (DAD) on various protocol layers of safety critical communication within such networks in detail. Thus, we provide such an analysis for ETSI ITS and WAVE. It shows that massive packet loss on various protocol layers can result from duplicated addresses. This effect is strengthened by close coupling between addresses on different protocol layers within current VANET approaches.

Incomplete knowledge of the whole network at a node leads to a variant of the well known hidden station problem affecting protocol addresses. This creates the need for a mechanism to detect and resolve duplicated addresses by stations not causing such a duplicate themselves. A mechanism for such external duplicate address detection and resolution is proposed. It does not rely on exchanging extra data sets like routing tables. Thus, the developed mechanism can be used in systems like WAVE, which do not use multi-hop communication and corresponding information exchange.

The provided evaluation shows that the problems obtained in the analysis actually happen, at the example of an intersection collision avoidance application. Furthermore, obtained results show the well usability of the taken approach. Thus, it should be considered for inclusion into future VANET standards.

Future work can study interaction between pseudonym changes required by duplicate address resolution and privacy enhancing cooperative pseudonym changing strategies.

References

[1] J. Harding, G.R. Powell, R. Yoon, et al., Vehicle-to-vehicle communications: readiness of V2V technology for application, Tech. rep. DOT HS 812 014, National Highway Traffic Safety Administration, Washington, DC, Aug. 2014.
[2] S. Rehman, M.A. Khan, T.A. Zia, L. Zheng, Vehicular ad-hoc networks (VANETs) – an overview and challenges, EURASIP J. Wirel. Commun. Netw. 3 (3) (2013) 29–38, http://dx.doi.org/10.5923/j.jwnc.20130303.02.
[3] C. Campolo, A. Molinaro, R. Scopigno (Eds.), Vehicular Ad Hoc Networks – Standards, Solutions, and Research, Springer, 2015.
[4] Intelligent Transport Systems (ITS); Security; Security header, certificate formats, June 2015.
[5] IEEE Standard for Wireless Access in Vehicular Environments, Security Services for Applications, Management Messages, Apr. 2013.
[6] K. Weniger, Passive duplicate address detection in mobile ad hoc networks, in: IEEE Wireless Communications and Networking, vol. 3, 2003, pp. 1504–1509.
[7] J. Petit, F. Schaub, M. Feiri, F. Kargl, Pseudonym schemes in vehicular networks: a survey, IEEE Commun. Surv. Tutor. 17 (1) (2015) 228–255, http://dx.doi.org/10.1109/COMST.2014.2345420.
[8] Intelligent Transport Systems ITS; Vehicular Communications, GeoNetworking; Part 4: Geographical addressing and forwarding for point-to-point and point-to-multipoint communications; Sub-part 1: Media-independent functionality.
[9] T. Buburuzan, et al., Draft C2C-CC standards system profile, Tech. rep., CAR 2 CAR Communication Consortium, v1.0.4 Jan. 2014.
[10] C.E. Palazzi, M. Gerla, M. Fazio, S. Das, Facilitating real-time applications in VANETs through fast address auto-configuration, in: 4th IEEE Consumer Communications and Networking Conference, 2007, pp. 981–985.
[11] R. Baldessari, C.J. Bernardos, M. Calderon, GeoSAC – scalable address autoconfiguration for VANET using geographic networking concepts, in: IEEE 19th International Symposium on Personal, Indoor and Mobile Radio Communications, 2008, pp. 1–7.
[12] S. Boudjit, C. Adjih, A. Laouiti, P. Muhlethaler, A duplicate address detection and autoconfiguration mechanism for a single-interface OLSR network, in: K. Cho, P. Jacquet (Eds.), Technologies for Advanced Heterogeneous Networks, in: LNCS, vol. 3837, Springer, 2005, pp. 128–142.
[13] IEEE Standard for Wireless Access in Vehicular Environments (WAVE) – Networking Services, Dec. 2010.
[14] N.H. Vaidya, Weak duplicate address detection in mobile ad hoc networks, in: ACM International Symposium on Mobile Ad Hoc Networking & Computing, 2002, pp. 206–216.
[15] S. Pietrowicz, et al., Vehicle segment certificate management using short-lived, unlinked certificate schmes, 2012.
[16] S. Bittl, K. Roscher, A.A. Gonzalez, Security overhead and its impact in VANETs, in: 8th IFIP Wireless Mobile Networking Conference, 2015, pp. 192–199.
[17] S. Bittl, B. Aydinli, K. Roscher, Effective certificate distribution in ETSI ITS VANETs using implicit and explicit requests, in: M. Kassab, et al. (Eds.), 8th International Workshop Nets4Cars/Nets4Trains/Nets4Aircraft, in: LNCS, vol. 9066, 2015, pp. 72–83.
[18] Intelligent Transport Systems (ITS); STDMA recommended parameters and settings for cooperative ITS; Access Layer Part (Jan. 2012).
[19] Intelligent Transport Systems (ITS); OSI cross-layer topics; Part 8: Interface between security entity and network and transport layer (Aug. 2014).
[20] K. Roscher, S. Bittl, A.A. Gonzalez, M. Myrtus, J. Jiru, EzCar2X: rapid-prototyping of communication technologies and cooperative ITS applications on real targets and inside simulation environments, in: 11th Conference Wireless Communication and Information, 2014, pp. 51–62.
[21] M. Behrisch, L. Bieker, J. Erdmann, D. Krajzewicz, SUMO – Simulation of Urban MObility: an overview, in: The Third International Conference on Advances in System Simulation, 2011, pp. 63–68.
[22] G.F. Riley, T.R. Henderson, The ns-3 network simulator, in: K. Wehrle, M. Günes, J. Gross (Eds.), Modeling and Tools for Network Simulation, Springer, Berlin, Heidelberg, 2010, pp. 15–34.

[23] A. Varga, Modeling and Tools for Network Simulation, Springer, 2010, pp. 35–59, Ch. OMNeT++.
[24] L. Cheng, B.E. Henty, F. Bai, D.D. Stancil, Highway and rural propagation channel modeling for vehicle-to-vehicle communications at 5.9 GHz, in: IEEE Antennas and Propagation Society International Symposium, 2008, pp. 1–4.
[25] D. Seydel, S. Bittl, J. Pfeiffer, J. Jiru, H. Beckmann, K. Frankl, B. Eissfeller, An evaluation methodology for VANET applications combining simulation and multi-sensor experiments, in: 2nd International Conference on Vehicular Intelligent Transport Systems, 2016, pp. 213–224.