Privacy Issues and Pitfalls in VANET Standards

Sebastian Bittl and Arturo A. Gonzalez
Fraunhofer ESK, Munich, Germany

Keywords: Privacy, Tracking, VANET, ETSI ITS, WAVE.

Abstract: Wireless vehicular networks are about to enter the deployment stage in the next years with important progress being made in Europe and the USA. Thereby, one of the core concerns is privacy of vehicles and their drivers, especially in Europe. Prior work has regarded only a small sub-set of the information exposed by current standards to an attacker for vehicle tracking. Thus, we take a close look on the data contained on different protocol layers of an ETSI ITS system. We find that much data is very distinctive and can be used to identify static vehicle parameters such as manufacturer or even model. This greatly reduces the usability of formerly proposed cooperative pseudonym switching strategies. Many more constraints have to be applied for selecting cooperation partners significantly reducing their availability. Therefore, current techniques cannot provide the level of privacy defined in VANET standards. Suggestions for improving the security entity and facility layer of ETSI ITS are given to limit the impact of the found issues.

1 INTRODUCTION

Wireless intelligent transport systems (ITS) are about to enter the mass marking in upcoming years. Important examples being ETSI ITS in Europe (MoU, 2011) and WAVE in the USA (J. Harding et. al., 2014). Thus, these systems' security and privacy aspects are gaining increased attention. Thereby, the possibility to track vehicles is a core point of concern, especially in Europe (Schütze, 2011). Many approaches for realizing such tracking exist. Typically, such attacks use the temporarily fixed pseudonym certificate, used by vehicles to authenticate their broadcast messages. However, higher level protocol information, e.g., identifiers or current position and velocity of a vehicle, is regarded for this purpose as well (Gerlach and Güttler, 2007).

Many studies have shown the possibility to track vehicles in ITS systems based on the mentioned data sets, e.g. (Tomandl et al., 2012). Therefore, a number of countermeasures has been published. These include context aware pseudonym changes (Gerlach and Güttler, 2007) and time synchronized pseudonym switching (Wiedersheim et al., 2010). Unfortunately, these mechanisms require the exchange of further messages between vehicles cooperating during the pseudonym change. This clearly increases the already significant overhead introduced by security mechanisms (see e.g., (Bittl et al., 2014)). Moreover, none of these works studies the influence of metadata contained in the security envelope of current ETSI ITS and WAVE systems on the privacy of vehicles. Additionally, only a fraction of the vast number of data fields from higher level applications is taken into consideration in prior work.

Our contribution focuses on the influence on the privacy of information broadcast by vehicles in ETSI ITS conforming VANETs. Thereby, we especially study the metadata contained in the security envelope of broadcast messages apart from the used pseudonym. Furthermore, we take a close look on the high number of data sets used by higher level protocols regarding their possibility to ruin the privacy efforts taken elsewhere. For the sake of compactness we focus the study of the ETSI ITS facility layer on Cooperative Awareness Messages (CAMs). However, much similarity between ETSI ITS and WAVE exists on the different protocol layers. Thus, we especially point out the cases which also apply for WAVE based systems.

The further outline is as follows. Section 2 reviews related work. Afterwards, Section 3 provides the in detail study of the impact of individual data fields on privacy of broadcasting vehicles. In Section 4, the achieved results are used to determine a metric for vehicle uniqueness within its vehicular environment. Finally, a conclusion is provided in Section 5 alongside with possible topics of future work.

Bittl S. and A. Gonzalez A..
Privacy Issues and Pitfalls in VANET Standards.
DOI: 10.5220/0005459101440151
In *Proceedings of the 1st International Conference on Vehicle Technology and Intelligent Transport Systems* (VEHITS-2015), pages 144-151
ISBN: 978-989-758-109-0

2 RELATED WORK AND ATTACKER MODEL

Recent work on privacy in vehicular area networks (VANETs) or intelligent transport systems (ITSs) includes (Gerlach and Güttler, 2007; Wiedersheim et al., 2010; Eichler, 2007; Scheuer et al., 2008; Buttyan et al., 2009; Tomandl et al., 2012). Basically, privacy in such networks relies on a pseudonym scheme which changes the identifiers (IDs) of a vehicle (or ITS-station (ITS-S)) on all protocol layers on a regular basis to avoid tracking (Schütze, 2011).

There are mainly two kinds of attacks on privacy in VANETs. Simple attacks just use identifiers like the station ID and a very limited set of additional information about the ITS-S, typically only the vehicle position. Advanced attacks include more context information for tracking, e.g., behavior of other vehicles (Gerlach and Güttler, 2007; Tomandl et al., 2012). Thereby, it has been shown that simple pseudonym change, like in ETSI ITS and WAVE, cannot avoid tracking. The probability of two (or even more) vehicles changing their pseudonym in close vicinity just by chance, confusing an attacker, is just to small.

Many approaches to confuse an attacker trying to track vehicles have been proposed. These apply concepts like *MixZones* (Scheuer et al., 2008), silent periods, *SLOW* (Buttyan et al., 2009), context aware pseudonym changes (Gerlach and Güttler, 2007) and time synchronized pseudonym switching (Wiedersheim et al., 2010) (see also (Tomandl et al., 2012) and references within). A common requirement of all these concepts is that vehicles must find indistinguishable partners in their vicinity with whom they cooperate to perform a secure pseudonym change. All vehicles should change all of their identification parameters together to confuse the attacker (Schütze, 2011). However, we show that finding such partners is quite unlikely to happen in VANETs using current ETSI ITS and WAVE standards.

A commonly assumed attacker model is the global passive adversary (Tomandl et al., 2012). This passive attacker can monitor all messages in the whole ITS system. This model is also assumed in the following.

Even advanced attacks from prior work (e.g., (Wiedersheim et al., 2010; Tomandl et al., 2012)) have so far not included usage of the biggest share of metadata from the security envelope and higher protocol level data from cyclic messages in VANETs following current standards. Thus, we study the usability of these data for more advanced attacks.

Properties of the studied standards from the ETSI ITS and WAVE families are explained in the next section alongside with their impact on privacy aspects.

3 DATA FOR VEHICLE IDENTIFICATION

ETSI ITS uses Cooperative Awareness Messages (CAMs) while WAVE utilizes Basic Safety Messages (BSMs) for the main data exchange in their VANET systems. Therefore, our focus is on the contents of theses messages on the different protocol layers.

When looking for possible privacy issues, the core focus is on data which differs for different groups of vehicles but is also constant for the individual vehicle over a long time. One example is vehicle dimensions which are identical for all vehicles of the same model but different for other models with high probability. We call that kind of data *volatile constant data*. In typical traffic scenarios many different vehicle types and models are present in the vicinity of a vehicle intending to perform a secure pseudonym change. To do so, the above described cooperative pseudonym strategies select partners whose broadcast information is as similar as possible to confuse the attacker. The presence of volatile constant data clearly makes it less probable to find such proper partners leading to possibly insecure pseudonym changes. Thus, the presence of such data should be avoided as far as possible.

Current standards bind the lifetime of MAC address, network layer address and station ID of the facility layer to the one of the pseudonym. This means, once the pseudonym gets changed the other identifiers get changed, too. Therefore, an attacker cannot profit from looking on more than one of these identifiers at once as they all provide the same temporarily valid information. Moreover, for the simple case of single hop broadcast, like it is used for CAM and BSM, the network and access layer do not add any information to the transmitted messages which can be used to track their senders.

In the next section metadata from the security envelope will be studied. Afterwards, the content of CAMs at the facility layer will be discussed.

3.1 Metadata in Security Envelope

The security envelope is used to secure content from the facility and network layer protocols by embedding them into a dedicated header and trailer, each consisting of different sub-parts. Thereby, content handed over to the security entity is treated in dependency of a so called security profile. These profiles determine the required header fields as well as the used cryptographic techniques, which can be digitally signing and/or encryption. The definition of the security envelope is quite similar in ETSI ITS (103, 2013) and WAVE (WAV, 2012).

In ETSI ITS the sets of mandatory header fields for security profiles *CAM* and *Generic* are subsets of the one for *DENM* (used for Decentralized Environment Notification Messages (DENMs)). Thereby, the location stamp in profiles *DENM* and *Generic* carries the same information as the vehicle position inside a CAM (103, 2013; 102, 2013b). Thus, this field is not discussed separately and the reader is referred to Section 3.2.1 for details.

We focus the further discussion on mandatory header fields from the CAM security profile. Privacy issues resulting from such fields are more severe than those from optional ones, as these can be simply skipped in practical implementations. In contrast, to fix issues regarding mandatory fields the standard has to be changed. Furthermore, (Nowdehi and Olovsson, 2014) suggests to remove the possible inclusion of optional fields. We support this proposal, as differing combinations of data sets in the envelope by different implementations clearly give an attacker a possibility to easily distinguish vehicles independently from their pseudonyms.

The following sections discuss the different header fields' privacy implications in detail.

3.1.1 Protocol Version

The used protocol version will be constant for all vehicles at the beginning of the deployment phase. However, over time it is very likely that multiple versions will be present in VANETs. As this value is constant for an individual vehicle over a long time, it is clearly volatile constant data. Thus, the presence of many different versions should be avoided even if they are otherwise compatible.

3.1.2 Security Profile

The content of this data field identifies the message type. In case all vehicles monitored by an attacker only send the same type of message, e.g., CAMs, he cannot discriminate the sender based on this data.

3.1.3 Signer Info

The signer information of a message may hold different contents. Thus the available information for the attacker differs. However, one can always uniquely determine the signer (and sender) of the message. Therefore, this is often called the pseudonym ID of the sender. In both CAM and BSM the field's content can either be the hash of the used pseudonym certificate (PSC) or the full certificate (103, 2013; WAV, 2012). Both systems use cyclic inclusion of the full certificate every 0.5 or 1 second, respectively. In case of security profiles DENM and Generic the full certificate is always present (103, 2013).

In case of an included PSC the following data is available to the receiver (103, 2013; WAV, 2012).

Signer Info of Pseudonym Certificates. A signer info field in a PSC identifies its signer which is an authorization authority (AA). This can be done either by a hash digest or by the full AA certificate. Both uniquely identify the AA. Current standards allow for a possible multitude of such entities to exist. In practice this will be probably done by the car manufacturers (OEMs). However, this leads to a privacy issue as the signer information is volatile constant data. An attacker can directly determine the OEM and use this to distinguish PSCs and thereby vehicles. PSCs signed by different AAs are very unlikely to be used by the same vehicle and a vehicle will very likely use only PSCs issued by the same AA. Obviously, vehicles of low volume OEMs will be particularly vulnerable.

To limit the usability of the AA's identity for an attacker one can think of mainly two countermeasures. Firstly, one could increase the number of AA certificates and make a single AA use a multitude of them. Thereby, the effort for an attacker to keep track of all certificates would increase. However, this would significantly increase the effort for AA certificate distribution to all ITS-S for a small security gain.

Secondly, one could limit the number of AAs. An ideal choice would be to have only one AA. This would clearly resolve the above described privacy issue completely, as an attacker cannot distinguish vehicles based on their used AA anymore. To implement this, OEMs would have to cooperate and use a common AA. As they plan to establish a common root certificate authority (CA) for Europe, this seems to be a usable approach. In order to limit the number of PSCs signed by a single AA certificate, one could significantly limit its lifetime. New ones can be deployed together with PSC updates.

Additionally, one should coordinate the lifetime of an AA's certificate with the lifetime of its issued PSCs. Thereby, any possibility to distinguish PSCs based on their signing AA should be ruled out. Moreover, the number of AA certificates to be stored securely inside the vehicles is kept (very) low.

Validity Restriction. The mandatory validity restriction of PSCs is a limited validity period. It is determined by a start and end time stamp. Both are used with an accuracy of one second. The PSC distribution scheme described in (WAV, 2012) and (102, 2010) defines that PSCs are delivered from an AA to an ITS-S upon request of the ITS-S. The remaining

details are implementation specific and not covered by the standard. However, a possible pitfall for privacy of pseudonym users exists which is caused by the mentioned time stamps.

This issue arises from the planned way of (re-)using PSCs in Europe. Thereby, each vehicle uses a pool of PSCs which are (re-)used until the full pool gets updated (Tomandl et al., 2012). The update period will probably be in the order of months.

A different approach is described in (J. Harding et. al., 2014) for the USA. Thereby, each PSC is only used once and the validity period is the order of minutes. However, this approach introduces significant overhead in the ITS system for PCS distribution. Either vehicles require frequent, reliable connections to the AA (or pseudonym certificate authority (PCA) (J. Harding et. al., 2014)) or a huge buffer filled with PSCs for future use. Even if the initially proposed validity period of five minutes gets doubled, this would still require a maximum amount of 144 PSCs per day. To protect the buffered PSCs, these have to be stored in secure memory, e.g., inside a Hardware Security Module (HSM). However, adding more memory to an HSM significantly increases its price. Moreover, many issued PSCs will stay unused as their validity period elapses while the vehicle is not in use. One would have to know the usage times of each vehicle in advance to avoid that, which is hardly practicable. Thus, the approach from (J. Harding et. al., 2014), while providing good privacy, probably bears too much overhead for large scale deployment.

An alternative approach for securing re-usage of PSCs is discussed in the following.

There are mainly two approaches for PSC generation inside the AA. Either the AA generates the PSCs upon request or the AA keeps track of the expiration of its users' PSCs to generate new ones in advance. In both cases a straight forward implementation would take the same time stamp (e.g., the current time at the AA) and use it as the common start validity time stamp of the signed PSCs. However, this means that all PSCs of a set delivered to an ITS-S have a very similar (or even the same) start validity time stamp. Thereby, making this information volatile constant data. Furthermore, this time stamp will be different with a very high probability for most cars as there is no timed synchronization of PSC requests.

The PSC users have no possibility to protect themselves against an attacker using validity time stamps for tracking them, as they cannot change the content of a PSC without invalidating its signature. Therefore, countermeasures have to be taken within AAs.

A straight forward solution would be to discretized the time stamps defining the validity period of PSCs. For example, all PSCs issued in one month could receive the start of this month as their start validity time stamp. The longer the discretization steps, the more vehicles will receive a set of PSCs with the same validity period. Thus the probability that multiple vehicles with common values in these data fields meet on the street increases removing the possibility to distinguish them.

Subject Attribute. The subject attribute field holds the subject type and public key of the PSC. This key is randomly generated and the subject type is fixed for all PSCs. Thus, there is no possibility to link PSCs based on this data set.

Subject Info. The subject info field holds a fixed value for all PSCs. Thus, it provides no possibility to track vehicles.

3.1.4 Generation Time

The generation time is individual for each message. However, the time difference between two sequential messages is clearly defined by the standard. Neither ETSI ITS nor WAVE define any change to the sending interval before or after a pseudonym change.

A common assumption is that clocks of ITS-S are well synchronized using GPS (Wiedersheim et al., 2010). Thus, time intervals between message generation of individual cars should be quite stable. Additionally, inside a group of cars the generation times of messages should be randomly distributed leading to an even distribution of used time stamps. Moreover, these time stamps are generated and transmitted with microsecond resolution (103, 2013). Thus, collisions in this data field confusing an attacker are unlikely. Hence, an attacker can track vehicles just on the generation time of their messages with high probability.

In case of BSMs the sending interval is fixed. For CAMs, it is determined by multiple parameters and can be in the range from 1 to 10 Hz. However, the current interval can be found in the transmitted CAM itself (102, 2013b). Thus, the attacker can easily use this information to avoid being confused by the variable sending interval of CAMs.

Furthermore, the time step is set at the network layer. Thus, the actual sending time being somehow randomized by the lower layer CSMA-CA scheme does not confuse the attacker.

We propose two solutions to overcome the described vulnerability. Both require the cooperating vehicles to use the same sending frequency before and after the pseudonym change for a minimum time span, e.g., one second. Firstly, one could reduce

the accuracy of the generation time to the maximum transmission interval being 100 ms for BSMs and 1s for CAMs. The security entity does not need to determine the sequence of received messages according to standards. Moreover, the validity time spans of PSCs are also given with full second resolution. Therefore, currently there is no need to use a high precision time stamp for the generation time of type *Time64* and it should be substituted by the lower resolution *Time32* type. A side effect would be to reduce the size of the security envelope by four bytes (103, 2013).

For the second solution, immediately after the pseudonym change the next sending must be delayed by a random waiting time. Its length should be in the order of the normal time difference between two successive transmissions. For example, for BSMs it would be between zero and 100 ms. Thereby, the attacker cannot determine the next generation time and gets confused. The impact on higher level applications should be low. From their perspective a maximum delay looks just like one missed message from the other vehicle.

3.1.5 Message Type

The message type field holds the same information as the security profile does. Moreover, the security entity does not need to distinguish different message types sharing the same security profile. Therefore, this field should be removed as it only adds overhead to the security envelope.

3.1.6 PSC Request List

An ITS-S requests up to six unknown PSCs by using the least three bytes of their hash values. Standard are unclear about when to remove entries from the request list. It should be flushed after a pseudonym change.

3.1.7 Trailer Field

There is only one type of trailer field in the standards. It holds metadata for interpreting the digital signature as well as the signature itself. Most parts of the trailer are fixed and the signature of multiple messages can only be linked together with the help of the respective public key. Therefore, the signature does not carry any additional privacy related information compared to the public key in the corresponding PSC (see Section 3.1.3 above).

Moreover, the encoding of the used ECC (elliptic curve cryptography) point may vary in general, but is probably constant for a particular vehicle. There are four options for the ECC point type field in the standard, with the core difference being enabled or disabled ECC point compression. With both choices used, this information is volatile constant data. In the worst case, with only two cars in a group and both using a different ECC point type, this information is already enough to render any pseudonym change useless. Thus, the standard should only allow only one option to be used. For other reasons to do so see (Nowdehi and Olovsson, 2014).

3.2 Data from Facility Layer

The CAM is defined as a deeply nested data structure (302, 2013). Thereby, an *ItsPduHeader* and a *CoopAwareness* field are present on the top level. The simple *ItsPduHeader* only holds basic information like the protocol version, message id and station id. These fields hold the same information as their respective counterparts in the security envelope. Therefore, their impact on privacy aspects is the same as for those data sets already described in Section 3.1.3.

The *CoopAwareness* field has two parts being the current generation interval (usable by an attacker as described in Section 3.1.4) and the *CamParameters* field consisting of several different containers. These are described in detail in the following.

3.2.1 Basic Container

The always present basic container holds the components station type and reference position.

Station Type. The station type associates the vehicle to some generic class, e.g., passenger car or light truck. This unchanging information is clearly volatile constant data.

Reference Position. The current position of the ITS-S measured at the vehicle's reference point (see (102, 2013a)) is available in each CAM. Prior work already showed that this information can be used to bypass simple pseudonym changes (Gerlach and Güttler, 2007; Wiedersheim et al., 2010). Therefore, the advanced pseudonym switching strategies suggested in these references should be used.

3.2.2 High Frequency Container

The high frequency container is part of every CAM. In case of an ITS-S being a vehicle the only used sub-part is a basic vehicle container. Parameters of the vehicle's current movement are given in this data set. These include heading, speed and driving direction. All these values can be used for advanced vehicle tracking (Gerlach and Güttler, 2007; Wiedersheim

et al., 2010). However, the remaining data inside this container has not been regarded in prior work.

Dimensions. The vehicle's dimensions length and width are given. According to (102, 2013b) the resolution is set to 0.1 meters. This value stays constant during one journey of a vehicle and thus it has to be regarded as volatile constant data. It is possible that the length of a vehicle changes from one journey to another, e.g., by extending it with a trailer. However, this is rare in practice especially for passenger cars.

To evaluate privacy aspects of broadcasting a vehicle's dimensions, we determined the number of different currently sold vehicle models in Germany. Then, we assigned them to the individual discretization steps of vehicle length and width. We took publicly available data from the German Kraftfahrt-Bundesamt (Kraftfahrt-Bundesamt, 2014) to obtain the share of different vehicle types, separated into OEMs and their models, on the overall traffic in Germany caused by new cars. Foreign cars traveling on German roads are excluded from this data set. However, it should still give a reasonable estimate about the distribution of models' dimensions. Moreover, we used public information from the 45 different OEMs present in (Kraftfahrt-Bundesamt, 2014) to obtain the individual dimensions of models.

We find that 73% of all vehicle models share a common combination of width and length with at least one other model. These cars have a market share of 75%. Thus, for a share of 25% one can determine the model directly given its discretized dimensions. Even the most populated set of vehicles with length 4.3 m and width 2.0 m includes only 17% of all cars.

Thus, distribution of vehicle dimensions clearly decreases the probability to find proper (i.e., indistinguishable) partners for a cooperative pseudonym change. Further discretization of the values to, e.g., 0.3 m would significantly improve the situation for many vehicles but can still not help the ones with outstanding dimensions and/or low penetration rates.

Dynamics. The parameters longitudinal acceleration, curvature (consists of curvature value and confidence), curvature calculation mode and yaw rate are included in the high frequency container. Thereby, the curvature calculation mode is again a value which is unlikely to change for an individual vehicle and may differ for different vehicles. Therefore, it should be regarded as volatile constant data.

The remaining values model a vehicle's trajectory. Many approaches for modeling and predicting such trajectories exists, e.g., (Ammoun and Nashashibi, 2009; Houenou et al., 2013). In case of pure tracking, i.e., no realtime interaction between attacker and vehicles, the attacker does not need to process the information in realtime. Thus, he can use computationally expensive but accurate and complex movement models. As we have seen above, the attacker can determine either the vehicle type directly or a group of possible vehicle types. This information can be used to tune the parameters of a movement model making it very accurate. Moreover, the prediction must only work well for a short time span as the CAM generation rate is at most one second.

To evaluate the impact of using an advanced movement model on the attackers ability to track vehicles one should use data obtained from real test drives instead of pure simulator output. This is because simulators like the well known SUMO use a predefined vehicle model. Therefore, tracking these simulated vehicles with a model which fits the one used to generate their movement will probably yield unrealistically high success rates. Further analysis of this issue is beyond the scope of this work and is a subject to future work.

Optional Data. Six more data sets may be optionally present in the container. Three of them (steering wheel angle, lateral, vertical acceleration) can be used to improve the movement model described above.

The remaining three values (acceleration control, lane position, performance class) each describe a vehicle's feature. These can be expected to change quite slowly, i.e., they should be regarded as volatile constant data. As all these fields are optional and can be added or removed individually, also the combination of sent data sets may differ between vehicles. Thus, usage of each extra value will increase the change that a particular vehicle uses a unique set of data inside its current vicinity. Thereby, it will strip itself from finding proper partners for a secure pseudonym change.

3.2.3 Optional Containers

In addition to the basic and high frequency container, the low frequency container is distributed cyclically, but not in every single CAM. It contains the vehicle role, exterior lights and path history fields. See (302, 2013) for details about inclusion rules.

In case of an uncommon vehicle role, e.g., rescue vehicle, the corresponding additional container is present in the CAM. The density of such vehicles in ordinary traffic is usually low. Thus, an attacker can easily track them just based on the presence of their dedicated containers in their CAMs.

Typically, the status of exterior lights changes slowly. Thus, it is volatile constant data.

The path history field should obviously be erased when a pseudonym change occurs or the inclusion rate of the container has to be such low that sequentially sent values of this field cannot be linked. Otherwise the attacker can simply link the pseudonyms based on this data. However, the current standards do not ensure such behavior.

4 VEHICLE UNIQUENESS

Secure pseudonym switching schemes from prior work are based on the assumption that broadcast data cannot be mapped to an individual vehicle except of the changed identifiers. We have shown in Section 3 that this is clearly not the case due to the presence of volatile constant data. To evaluate the impact of our findings on vehicle privacy we introduce the metric of *vehicle uniqueness (VU)*. It measures how much a particular vehicle differs from its vehicular environment regarding data observable by an attacker.

Prior work showed that tracking of vehicles becomes more difficult alongside with higher traffic density and longer distances traveled during a cooperative pseudonym switching maneuver (Tomandl et al., 2012). However, this only holds in case the attacker has no extra information for re-identification of vehicles after a pseudonym change. VU is a metric for the availability of such extra information. In case a vehicle is unique inside the area of pseudonym switching the attacker can always track it, independently of the used pseudonym switching algorithm.

To calculate VU an exposed feature vector e_i holding all available volatile constant data is assigned to each vehicle. Thereby, $i \in I$ relates to a particular vehicle within a group of vehicles I ($|I| \geq 1$) cooperating during a pseudonym change. VU is defined by

$$VU = \Pr\{|\{x|e_x = e_y; x \neq y; x, y \in I\}| = 0\} \ .$$

This means that $VU \in [0;1]$ is the probability that there is just one car within I having one particular exposed feature vector. Such vehicles are indistinguishable for an attacker in regard to volatile constant data.

In the following, we take three different pseudonym switching schemes into regard. These are

1. uncoordinated pseudonym switching (ETSI ITS and WAVE) with $|I| = 1$ with high probability,
2. mix zones with $|I|$ depending on traffic flow and size of the mix zone and
3. silent periods with $|I|$ depending on traffic flow and length of silent periods.

Moreover, we include the following data into e_i:

- AA of PSCs, we assume one AA per OEM and
- vehicle dimensions (see Section 3.2.2).

We assume that all cars from the same OEM use the same encoding of ECC points (see Section 3.1.7). Thus, this data does not influence VU in our case and is not regarded further. The rest of the volatile constant data sets from Section 3 are assumed to be identical for all cars. This leads to a best case assumption for privacy of vehicles. Moreover, we assume that the probability of two cars within I sharing a common value of e_i ($|e_i| = 3$) only depends on the share of their particular model within the set of all vehicles.

We use the vehicle distribution from (Kraftfahrt-Bundesamt, 2014) to estimate VU. Moreover, an analysis of vehicle dimensions for the models of different OEMs (see also Section 3.2.2) shows that the data included in e_i allows to uniquely identify the model of a vehicle, e.g., as VW Golf VII, from a single CAM including the PSC. Thus, one can calculate the probability to encounter a vehicle with a particular e_i from the mentioned vehicle distribution data set.

The number of vehicles encountered during a pseudonym switching maneuver $|I|$ is varied by varying the traffic flow (given in $\frac{vehicles}{kilometer}$) and size of mix zones or length of silent periods, respectively. The traffic density is varied from 16 to 45 $\frac{vehicles}{kilometer}$ per lane following (Gerlach and Güttler, 2007) to represent low volume traffic as well as a jammed setup. We use the parameter set from (Tomandl et al., 2012) for the size of mix zones (25m - 400m), length of silent periods (1250ms - 20s) and velocity range (0 - 250 $\frac{km}{h}$). The obtained results are given in Figure 1.

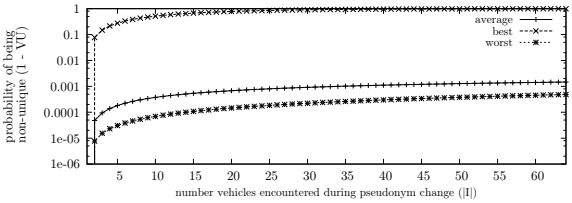

Figure 1: Vehicle uniqueness during pseudonym change.

Thereby, the *best* case relates to the most common car model. It is obviously the least unique one within the set of all vehicles. However, only about 7.7% of all vehicles can profit from the good results for this model having a high chance to find indistinguishable partners for a cooperative pseudonym change. Moreover, the *worst* case relates to the least common car.

One can see from Figure 1 that the value of $1-VU$ increases alongside with $|I|$. However, for an *average* vehicle it is very low for all regarded values of $|I|$. However , combinations of high velocity and high

traffic flow, leading to high values of $|I|$, rarely occur in practice. Thus, VU will exceed 99.9% in most real world scenarios with moderate traffic flow.

Higher values of $|I|$ than the ones used above would relate to unrealistically high traffic flow or extending the size of mix zones and length of silent periods to values rendering higher level ITS-applications unusable (Tomandl et al., 2012). Calculation of VU is independent of the pseudonym switching strategy, but the achievable size of $|I|$ differs. While cooperative PSC switching strategies can adjust it, uncoordinated ones, e.g., from ETSI ITS or WAVE, cannot do so.

The obtained results show that even without other tracking mechanism an attacker can track a vehicle with high probability using just a small set of constant volatile data, even though the vehicle performed a pseudonym change. This shows that the presence of volatile constant data is able to render PSC changes useless, as an attacker can re-identify vehicles using this data after the pseudonym change. Combining this attack with further tracking mechanisms, e.g., from (Tomandl et al., 2012), promises to achieve very high tracking probabilities. Thus, the mechanisms for avoiding volatile constant data in VANET messages suggested in Section 3 should be used to limit the trackability of vehicles.

5 CONCLUSIONS AND FUTURE WORK

With upcoming deployment also privacy aspects of VANETs gain increased attention. Therefore, we studied the influence of information currently present in ETSI ITS and WAVE standards on proposed privacy protecting pseudonym usage strategies.

Thereby, we find that the main requirement of pseudonym change strategies, the cooperation of multiple indistinguishable vehicles, is unlikely to be found in practice with current standards being in use. Multiple suggestions have been made to improve this situation, which require to adjust the standards.

Future work can implement the outlined tracking mechanisms in a simulation environment to study the influence of parameters like CAM generation rules.

REFERENCES

(2010). Intelligent Transport Systems (ITS); Security; Security Services and Architecture. V1.1.1.

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

(2012). Draft Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages. P1609.2, D12.

(2013a). Intelligent Transport Systems (ITS); Facilities layer function; Facility Position and time management. V0.0.2.

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

(2013b). Intelligent Transport Systems (ITS); Users and applications requirements; Part 2: Applications and facilities layer common data dictionary. V1.1.1.

(2013). Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service. ES 302637-2, V1.3.0.

Ammoun, S. and Nashashibi, F. (2009). Real time trajectory prediction for collision risk estimation between vehicles. In *IEEE ICCP*.

Bittl, S., Gonzalez, A. A., and Heidrich, W. (2014). Performance Comparision of Encoding Schemes for ETSI ITS C2X Communication Systems. In *VEHICULAR*, pages 58–63.

Buttyan, L., Holczer, T., Weimerskirch, A., and Whyte, W. (2009). SLOW: A Practical pseudonym changing scheme for location privacy in VANETs. In *IEEE Vehicular Networking Conference*, pages 1–8.

Eichler, S. (2007). Strategies for Pseudonym Changes in Vehicular Ad Hoc Networks depending on Node Mobility. In *IEEE Intelligent Vehicles Symposium*.

Gerlach, M. and Güttler, F. (2007). Privacy in VANETs using Changing Pseudonyms - Ideal and Real. In *IEEE VTC*, pages 2521–2525.

Houenou, A., Bonnifait, P., Cherfaoui, V., and Yao, W. (2013). Vehicle Trajectory Prediction based on Motion Model and Maneuver Recognition. In *IEEE IROS*, pages 4363–4369.

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 Safty Administration.

Kraftfahrt-Bundesamt (2014). Neuzulassungen von Personenkraftwagen im August 2014 nach Marken und Modellreihen. online: 10.01.2015.

Nowdehi, N. and Olovsson, T. (2014). Experiences from Implementing the ETSI ITS SecuredMessage Service. In *IEEE IVS*, pages 1055–1060.

Scheuer, F., Plößl, K., and Fedrrath, H. (2008). Preventing Profile Generation in Vehicular Networks. In *IEEE WiMob*, pages 520–525.

Schütze, T. (2011). Automotive Security: Cryptography for Car2X Communication. In *Embedded World Conference*.

Tomandl, A., Scheuer, F., and Federrath, H. (2012). Simulation-based Evaluation of Techniques for Privacy Protection in VANETs. In *IEEE WiMob*, pages 165–172.

Wiedersheim, B., Ma, Z., Kargl, F., and Papadimitratos, P. (2010). Privacy in Inter-Vehicular Networks: Why simple pseudonym change is not enough. In *WONS*, pages 176–183.