A Decentralized Group Privacy Protocol for Vehicular Networks

Hagen Stübing1, Marco Pfalzgraf2, and Sorin A. Huss3

1General Motors Europe, Active Safety, Germany, hagen.stuebing@gm.com
2Vector Informatik GmbH, Embedded Software, Germany, marco.pfalzgraf@vector.com
3Technische Universität Darmstadt, Integrated Circuits and Systems Lab, Germany, huss@iss.tu-darmstadt.de

Abstract—Vehicular Networks by means of Car-to-X (C2X) communication aims to enhance road safety and traffic efficiency by exchanging foreseen traffic information. For successfully establishing this technology on the market, C2X messages have to be secured and the driver’s privacy must not be violated. However, currently applied pseudonymization strategies provide only basic protection against profiling and are entirely ineffective towards a powerful global adversary. We present a novel group privacy protocol, which creates dynamic cryptographic ‘Mix Zones’ in a decentralized and cooperative way. The proposed protocol obfuscates pseudonym changes and thus reduces traceability of vehicles significantly. While geographical cells are used to establish a secret group key among all members, the group is maintained even when travelling along the road. Using the group key, a vehicle is able to send secure authenticated messages, though its anonymity is preserved. We simulate the proposed protocol by means of a dedicated C2X simulator and evaluate the achieved privacy enhancements with respect to a global passive adversary.

I. INTRODUCTION

Vehicular Networks based on Car-to-Car and Car-to-Infrastructure communication (Car-to-X, C2X) recently have gained great momentum as several Field Operational Trials, like simTD [1] or DriveC2X [2], have started and the standardization work by IEEE and ETSI [3] is reaching a deployable state. In the scope of current work towards a reference architecture for Intelligent Transportation Systems (ITS), ETSI has defined a basic set of messages for safety related information exchange. Among others these are Cooperative Awareness Messages (CAMs), which include a vehicle’s mobility data in terms of position, speed, and heading and are sent within intervals from 1s to 100 ms [3].

In order to make Car-to-X a success, the transmitted data has to be reliable and thus secured by appropriate measures. For this purpose, a major trend towards using a Public Key Infrastructure can be identified. In this context signatures are aimed to authenticate messages. The used public keys are to be certified by a certification authority (CA). Furthermore, to yield customer acceptance, the privacy of the driver has to be preserved in any case. Apparently, the high spatial and temporal resolution of the transmitted mobility data within CAMs allows a precise tracking of vehicles, which represents a threat to the driver’s privacy and consequently has to be obstructed. Although there are currently no dedicated standards available, which would define measures to reduce linkability in C2X, a commonly accepted concept based on pseudonymization has been established. In order to reduce linkability, a vehicle owns several certificates with limited lifetimes, which are frequently changed during communication. In the context of privacy those anonymous certificates are referred to as “pseudonyms”.

However, when applying traceability as a metric, currently deployed pseudonymization strategies, like, e.g., in simTD [4], provide only a low privacy protection against attacks of a global adversary. Using temporal and spatial relations between two succeeding locations of a vehicle, the old and new pseudonyms can be related to each other. Assuming a powerful adversary, which has access to all sent messages of the target vehicle, a maximum sampling rate of 1Hz is already sufficient to successfully resolve most of the pseudonym changes [5].

From the previous discussion we conclude that simple pseudonym changes do not provide a sufficient privacy protection against correlation attacks and, consequently, further investigations on privacy enhancing technologies have to be carried out. In this work we present a novel approach for obfuscating pseudonym changes based on dynamic Mix Zones. We first propose a group protocol, where a common group key is assembled based on multiple key fragments obtained from all group members. Then we validate the performance of the proposed protocol under the assumption of a global passive adversary and analyze the gained privacy enhancements compared to simple pseudonym changes.

The paper is structured as follows: In section II we summarize and discuss several known approaches for establishing Mix Zones for C2X communication. We derive the fundamental C2X group protocol requirements in section III. In section IV we introduce the underlying system model and the protocol parameters. Then, in section V, the protocol specification is given. In section VI the advocated privacy protocol is evaluated for its effectiveness. Finally, in section VII we conclude the paper and give some remarks on future work.

II. RELATED WORK

The concept of Mix Zones has been first applied to vehicular networks in [6]. Accordingly, a Mix Zone is defined as a geographical area, where vehicles are not observable by possible adversaries, and thus can change their pseudonym without being tracked. Mix Zones in vehicular networks can be categorized into two distinct classes: Situational Mix Zones and Cryptographic Mix Zones.
The AMOeba [7] concept represents a Situational Mix Zone and proposes Silent Periods for C2X. When entering a network a vehicle changes its pseudonym and remains silent for a randomly chosen period of time. If neighboring vehicles update their pseudonyms at the same time, the probability for tracking is possibly reduced. We argue that without inter-vehicular synchronization and a rather low change frequency like currently deployed in simTD [4], the likelihood of two vehicles changing pseudonyms at exactly the same time and location is far too low to impede tracking.

In [8] a Cryptographic Mix Zone (CMIX) protocol is proposed, where vehicles switch to symmetric cryptography every time they enter the communication range of a Road Side Unit (RSU). The CMIX protocol is exercised to distribute a symmetric key from the RSU to every authenticated vehicle. Having a symmetric key enables the vehicles to send encrypted messages while staying in the Mix Zone. Although this approach is promising, we argue that a comprehensive covering of all intersections with RSUs is not realistic due to high financial costs. Especially during an early deployment phase, RSUs with backend connectivity are very likely to be installed only on few intersections with a high traffic volume. In [9] we presented a further decentralized privacy protocol based on n-party Diffie Hellman scheme, which obfuscates pseudonym changes by means of dynamic Mix Zones.

III. PROTOCOL OBJECTIVES

In the following we state the major requirements a group privacy protocol has to fulfill in order to be in line with safety and security demands.

1) Privacy Enhancements: Obviously, the main objective of any privacy protocols lies within the enhancement of the drivers’ anonymity. In this context we measure anonymity by means of unlinkability.

2) Decentralization: The CMIX protocol [8] relies upon a trustworthiness of RSUs to establish Mix Zones. Having a centralistic instance, which is in charge of all protocol parameters (e.g., symmetric keys), weakens the privacy protection. For instance, in case of the CMIX protocol, no privacy towards the RSU operator can be ensured. Concentrating the key generation in a single station violates the peer nature of the group, because trust is getting centralized and key agreement is being replaced by key distribution. We argue that a centralistic instance always represents a single-point of failure and is an attractive attack target for any adversary. Instead, for cryptographic Mix Zones, a decentralized way of creating and maintaining the group is preferable.

3) Robustness: Due to shadowing effects messages might get lost, a situation which has to be taken into account for any protocol design. We require the privacy protocol to cope with message losses and the high mobility of communication nodes.

4) Flexibility: C2X networks are highly dynamic, i.e., vehicles may enter and leave the network spontaneously and unannounced. Consequently, besides the initial group establishment, further mechanisms to manage the group have to be defined. Among others, these mechanisms have to include protocols for vehicles to join and disjoin the group.

5) Efficiency: As the bandwidth of the C2X communication channel is limited and primarily dedicated for exchanging safety related information, we require any privacy protocol to keep the communication overhead as low as possible.

6) Safety-Preserving: Establishing a privacy solution at the expense of the C2X safety functionality has to be avoided. Although we are aware that certain implications cannot be fully circumvented, a trade-off has to be found in a way that safety use cases can still work properly to serve their purpose.

7) Accountability: Designing a privacy solution that provides privacy against authorities is risky, since legislation might always overrule the design and requires a change of the entire architecture. Lawful interception might become a major issue in case of severe traffic accidents, where C2X messages might become legally binding.

IV. SYSTEM MODEL AND REQUIREMENTS

This section describes the underlying system model and prerequisites for carrying out the proposed privacy protocol. The protocol presented in this work is built on top of the common C2X architecture as deployed in [10]. Data Security is ensured by means of a PKI, which foresees digital pseudonym certificates (Cert) and signatures to verify the trustworthiness of all sent messages. Additionally, every vehicle is provided with a symmetric key $k_{CA}^{Sym}$. The symmetric key is only known by the vehicle and the CA and is involved to implement the requirement for accountability during the group phase.

The advocated novel key fragment protocol is executed in a cooperative manner, which demands every participant to be aware of all additional protocol parameters. In particular, those protocol parameters are related to the spatial and temporal synchronization during the group formation process.

A. Spatial Synchronization

Especially for the group setup a measure for defining all initial group members has to be given. For our purpose of creating cryptographic Mix Zones a geographical measure seems to be a natural choice. In order to meet the requirement of decentralization, we apply an approach similar to the cell concept introduced in [11].

![Figure 1: Cell concept and protocol parameters](image-url)
Accordingly, a group is defined by all vehicles located in a cell. To serve our purpose, we redefine cells to be non-overlapping and introduce a separation (Cell-Distance) between neighboring cells as depicted in Figure 1. Every cell holds a unique identifier (Cell-ID) and geographical position (Cell-Pos), which are both known parameters to all vehicles. The cell size (Cell-Radius) is defined as a constant and therefore does not have to be attributed to every cell separately. For our implementation we assume that cell parameters are available from a database inside every vehicle. Selecting the right dimensions and locations of cells is essential for the effectiveness of the proposed privacy protocols. On the one hand, the cell radius should be as large as possible in order to ensure a maximum number of group members. On the other hand, the maximum dimension of a cell is limited by the vehicles’ communication range of approximately 500-600 meters [1]. This threshold comes from the necessity that all vehicles within one cell have to be able to communicate with each other to successfully create and exploit a common group key. As a trade-off, we define a cell radius of approximately half the communication range to meet both requirements. In order to avoid interference between cells, we define a minimum separation of 1200 meters such that there is no cross-talk between groups of neighboring cells.

### B. Temporal Synchronization

Forming a group and dissolving it again is a cyclic process, which has to be synchronized among all participating vehicles using UTC (Coordinated Universal Time) time. In Figure 2 different group phases are exemplarily shown for a single cell.

<table>
<thead>
<tr>
<th>Notation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$t_{\text{Start}}$</td>
<td>starting time for group establishment</td>
</tr>
<tr>
<td>$d_{\text{group}}$</td>
<td>setup interval to establish group key</td>
</tr>
<tr>
<td>$k_i$</td>
<td>asymmetric private key of vehicle $i$</td>
</tr>
<tr>
<td>$Cert_i$</td>
<td>certified public key of vehicle $i$, (pseudonym)</td>
</tr>
<tr>
<td>$\text{Sig(CAM; } k_i \text{)}$</td>
<td>signed data, using $k_i$, (ECC224)</td>
</tr>
<tr>
<td>$\text{KeyFrag}_i$</td>
<td>16 bit random number of vehicle $i$</td>
</tr>
<tr>
<td>$E(\text{data; Cert}_i)$</td>
<td>encrypted data using $\text{Cert}_i$</td>
</tr>
<tr>
<td>$k_{\text{CA}}$</td>
<td>symmetric CA key of vehicle $i$</td>
</tr>
<tr>
<td>$k_{\text{group}}$</td>
<td>symmetric group key</td>
</tr>
<tr>
<td>$\text{HMAC(\text{data; } k_i)}$</td>
<td>Hash Message Authentication Code of data using key $k_i$</td>
</tr>
</tbody>
</table>

#### V. Key Fragment Group Protocol

A. **Group Establishment**

In this section the process for establishing a group key by means of key fragments is presented. The protocol anticipates four successive phases, which are repeated at every starting time point $t_{\text{Start}}$.

1) **Initial Group Definition**

During the Initial Group Definition phase vehicles are frequently broadcasting CAMs, which are used by surrounding vehicles to determine which neighbors are located in the cells. In Figure 3 a basic scenario is illustrated, where at the starting time $t_{\text{Start}}$ vehicle A, B, and C are located within a cell, whereas vehicles X, Y, and Z are located outside the cell. In Table 1 the related notations are summarized.

<table>
<thead>
<tr>
<th>Notation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\text{CAM}$</td>
<td>Group Establishment</td>
</tr>
<tr>
<td>$\text{KeyFrag}$</td>
<td>16 bit random number of vehicle $i$</td>
</tr>
<tr>
<td>$\text{E(\text{data; Cert}_i)}$</td>
<td>encrypted data using $\text{Cert}_i$</td>
</tr>
<tr>
<td>$\text{Cert}_i$</td>
<td>symmetric CA key of vehicle $i$</td>
</tr>
<tr>
<td>$k_{\text{group}}$</td>
<td>symmetric group key</td>
</tr>
<tr>
<td>$\text{HMAC(\text{data; } k_i)}$</td>
<td>Hash Message Authentication Code of data using key $k_i$</td>
</tr>
</tbody>
</table>

Given the cell center and radius every vehicle can determine whether it is located inside a cell or not. The cell concept serves as a kind of geographical “stamp” to mark initial group members at starting time. In the following procedure the marked vehicles A, B, and C do not necessarily remain in the cell to successfully complete the initialization process.

#### Figure 3: Scenario at the starting Time $t_{\text{Start}}$ of the Group

2) **Key Fragment Distribution**

As a result of the previous phase, vehicle A, B, and C have been selected to create a group and are instantly starting to distribute key fragments. In the context of this protocol we define a key fragment $\text{KeyFrag}$, as a confidential 16-bit random number, which is created individually in every vehicle. To assemble the common group key, each fragment has to be communicated among all group members via a secure channel. Hence, all key fragments have to be encrypted by means of asymmetric cryptography before sending.

For instance, in our accompanying example in Figure 3, vehicle A requires the key fragments from vehicle B and C and in turn sends its encrypted key fragment to them, respectively. From the previously received CAMs, vehicle A can extract vehicle B’s and C’s certificate and uses the included public key to send the encrypted key fragment.
Because only the receiver holds the related private key, he will be able to decrypt the message. To meet previously stated requirements for low message overhead, we propose to include the encrypted key fragments into the payload of the next regularly sent CAM broadcast. In Figure 4 the message exchange during the group establishment phase is illustrated.

3) Group Key Generation
After completion of the previous phase all vehicles are aware of the same set of key fragments. These key fragments are then aggregated to a common group key $k_{\text{group}}$. By including the Cell-ID and starting time $t_{\text{start}}$, the resulting group key now features both a spatial and a temporal dependency. This way the likelihood of group key correlation is reduced for the cases, where the same vehicles are initiating a new group at some other point in time. The group key generation function is further detailed in the implementation section of this paper.

4) Anonymous Message Exchange
After key establishment, vehicles continue signing messages using the symmetric group key $k_{\text{group}}$. In doing so, both objectives are met at the same time: a reliable authentication of messages, while the anonymity of the sender is maintained. We advocate an usage of the Keyed-Hash Message Authentication Code (HMAC-256) that is approved by the NIST to provide message authentication. Accordingly, every sender creates an unique hash value from the message content, which cannot be reproduced without knowledge of the symmetric group key.

Besides creating a HMAC for integrity checks within the group, every vehicle additionally employs a second HMAC computed with symmetric CA key $k_{CA}^A$. By means of this second HMAC the CA can confirm, if a given message has been sent from a certain vehicle. Any bit manipulation of the message or the attached HMAC performed by an adversary will be detected by the CA. Furthermore, in order to be able to use the second HMAC for accountability purposes, we require the HMAC creation to be performed within a tamper proof module inside every vehicle.

In Figure 5 the exchanged messages right after the group establishment phase are depicted. Vehicles A, B, and C are broadcasting CAMs, which are authenticated using symmetric cryptography, whereas vehicles X, Y, and Z rely upon asymmetric cryptography. In order to overcome interoperability problems at the border of a group, join mechanisms have to be defined, which allow transferring the group key to non-members as well. Related methods are detailed in the following section.

Figure 4: Secure Key Fragment Exchange

Figure 5: Anonymous Message Exchange within the Group

B. Group Management
This section is dedicated to group maintenance. In particular, we establish how new vehicles can be integrated into the group and how interference between adjacent groups can be handled.

1) Group Join
Immediately after the group establishment process, vehicles in the vicinity have to join the group for reasons of interoperability. Like before, authentication towards the group is implicitly realized by evaluating the certificate of received CAMs. Non-members, like vehicle X in Figure 6, can migrate to the group by requesting the group key. In response, a close group member (e.g., vehicle A) is encapsulating the group key $k_{\text{group}}$ and the group starting time $t_{\text{start}}$ into a message. Signing the message with the forwarder’s pseudonym is necessary to ensure authenticity. The entire reply-message is encrypted using the certificate of vehicle X for keeping the group key as well as the sender identity confidential to the adversary. Note that the reply-message of vehicle A does not include any mobility data (i.e., position, speed, and heading). Hence, if vehicle X still can verify the overall authenticity, but cannot reveal the sender’s identity using spatial-temporal information. In this way privacy of group members is preserved, even when answering to group joins.

Figure 6: Group Join Protocol

2) Group Interference
The previously presented Join protocol allows extending the group beyond its initial group size. Groups are expanding
into all directions simultaneously and, possibly, at some point in time they will interfere with adjacent groups. Group interference might also be caused by single vehicles, which are traveling faster than other group members and are therefore reaching some other group ahead. If vehicles of different groups meet, those vehicles which are located inside the interference area instantly will leave the group. They continue sending messages with their regular pseudonym and are requesting the unknown group key of the adjacent group. Having received the respective group keys allows those intermediate vehicles to verify messages sent by both groups. However, instead of using a group key, those vehicles use their own pseudonym to authenticate messages. For those vehicles no anonymity is provided by the group anymore. We consider this trade-off as most appropriate since it includes the lowest complexity at an acceptable privacy level for the remaining group. In Figure 7 the resulting scenario is illustrated, where vehicle A and B serve as a sort of buffer to separate both groups.

![Figure 7: Group Interference](image)

3) **Group Disjoin**

If a vehicle has to disjoin a group, it switches over to one of its own pseudonyms for signing subsequent messages. A notification to other group members is not required. In general, there might be two reasons for disjoining a group: Either the group lifetime $d_{\text{group}}$ has exceeded and the entire group is dissolving, or the vehicle has left the communication range of the other group members.

C. Implementation

While the previous section gave a more general overview of the proposed key establishment protocol, in this section the implementation is further detailed by means of decision flow graphs as depicted in Figure 9. At every starting time point $t_{\text{start}}$ the host vehicle instantly queries the internal cell database to get the location of the cell closest to its own position. If at starting time the host vehicle was located inside the cell, it forms a group with its neighbors (D1). For that purpose each vehicle calculates the Member Set, which is defined as a list including all vehicles from which the host vehicle assumes that they are taking part in the group establishment process. The Member Set is determined by iterating the neighborhood table, which includes received last positions of all surrounding vehicles. Because of deviating timestamps the entries do not necessarily reflect the precise scenario at starting time. To bring all entries down to a common time basis, linear approximation is used to find the location of all vehicles at starting time and the Member Set is defined accordingly. However, inconsistent member sets between group participants cannot be fully excluded as there always remains space for some errors due to the high mobility of the network. Those different member sets will result into an inconsistent calculation of the group key among the group members. To solve this issue, we are proposing a basic voting scheme for defining the group members. Accordingly, every group member communicates its own “view on the group” to all surrounding neighbors. By adding a vehicle’s own Member Set to every outgoing message, a common awareness between all group members can be established. The given approach ensures that every member determines the greatest common subset among all Member Sets.

![Figure 8: Detailed Message Format for Vehicle C](image)

![Figure 9: Group Decision Flow Graph for Sender and Receiver](image)

Due to message loss and shadowing effects key fragments might get lost. In order to cope with such effects, we extend the protocol, which allows requesting of missing key fragments by attaching Request Sets to every message. In Figure 8 the detailed packet structure as sent by vehicle A is illustrated exemplarily. The concept of Request Set has been introduced not only to enable reliable key fragment exchange. It furthermore ensures that the point in time, where all vehicles are entering the group mode, is synchronized among all members. As long as any member is still sending a non-empty Request Set, none of the other group members is switching to the group key to sign messages.

VI. SIMULATION AND EVALUATION

The following evaluation has been carried out to analyze the privacy protocol with respect to its technical feasibility, temporal behavior, and anonymity achievements. State-of-the-art simulators are used to study the protocol behavior under...
realistic traffic scenarios and vehicle movements. The technical feasibility is mainly influenced by the mobility of the group members. In particular, we want to evaluate whether the proposed protocol has been specified accurately enough to guarantee reliable group establishment and maintenance. By observing the behavior of the group over time, we obtain protocol characteristics like the duration for group establishment or the point in time until group interferences appear. Protocol parameters like cell distances and group lifetime heavily depend upon the actual road geometry. In the following we shape those parameters to be appropriate for an exemplary case study. Similar simulations will have to be carried out for every other road section, on which the privacy protocol is going to be deployed.

A. Simulation Setup

For simulating the proposed privacy protocols we use VSimRTI [12], which is a flexible and light weight framework for dynamically simulating Car-to-X communication scenarios. VSimRTI enables the coupling of different simulators for evaluating traffic flow and wireless communication as well as dedicated C2X applications. Some of the most common simulators are already part of VSimRTI: SUMO for traffic simulation and JIST/SWANS for wireless communication simulations. As an example scenario we selected a motorway with three lanes in the area around Berlin. For our analysis we studied the protocol behavior with respect to three different vehicle densities as classified by FGSV – the German research agency for roads and transport [13]:

- < 16 vehicles/km low traffic density
- 16 - 32 vehicles/km medium traffic density
- 32 - 45 vehicles/km high traffic density

We defined three different vehicle types with velocities of 80 km/h, 110 km/h, and 130 km/h, respectively. These values represent the maximum speed a driver tends to drive if traffic conditions are suitable. All three vehicle types are equally distributed. Vehicles adapting their driving behavior according to the traffic situation, e.g., they are keeping a safe distance from the skiers ahead and are overtaking other vehicles if the fast lane is free.

B. Temporal Behavior Evaluation

Simulations of the privacy protocol have been performed for three different cell distances, namely 1900 m, 2600 m, and 3200 m, respectively. The entire protocol has been implemented as specified in previous sections. The diagrams in Figure 10 to Figure 12 display the observed behavior. As an initial setting, we restrict the group lifetime to 10 seconds. Within those diagrams, the following data is illustrated over time:

- **Generating Group Members:** This graph indicates how many vehicles are located in the cell during the starting time and are creating the group key. The number of generating vehicles is increased every time one of the initial group members has received all necessary fragments and can start generating the group key.

- **Joining Vehicles:** This curve shows how many vehicles are joining the group via the presented join protocol over time.

- **Disjoining Vehicles:** Vehicles spontaneously may leave the group because of the previously stated reasons. We measured the point in time when a vehicle stops sending message authenticated with the group key and switches over to an own pseudonym.

- **Group Size:** This curve indicates the actual group size and includes all vehicles, which are currently sending anonymized messages via the group key. Together with the curves for joins and disjoins this curve essentially provides information on how stable the group formation is.

In Figure 10 the averaged observations of the first simulations for a cell separation of 1900 m are summarized. Accordingly, in this simulation it takes less than 1 second for the initial group members to exchange all key fragments and to create the group key. Note that the first vehicle has already generated the group key after 0.5 seconds. This short time period enables this vehicle to already reply to join requests of non-members, while other group members are still collecting key fragments. This explains the strongly increasing number of “joins” right after the group establishment phase ($d_{setup} = 1$ second). With respect to interoperability issues, this represents a desirable effect. After 2 seconds the first group members are coming into contact with another group and are disjoining the group according to the previously described protocol for group interference. From then on the entire group remains stable at a group size of about 15 vehicles until finally it is dissolved again. As a conclusion, we observe that for a medium vehicle density of 23 vehicles/km and a cell separation of 1900 m the group reaches its maximum size after 2 seconds. This time interval therefore indicates the recommended minimum group lifetime $d_{min}$ a group has to be maintained on that road segment.

The curves depicted in Figure 11 and Figure 12 reflect the averaged measurements taken for a cell distances of 2600 m and 3200 m, respectively. As expected, the minimum group lifetime increases for larger cell distances. For a cell separation of 2600 m we require a lifetime $d_{min}$ of 3 seconds and for 3200 m a lifetime of 6 seconds. Based on the previous observations we summarize our results:

- The initial group establishment process is completed within the timeframe of one second. The duration varies only slightly for different vehicle densities.

- With increasing cell distances the total number of group members is increased while the number of early disjoins is decreased.

- Vehicle densities and cell distances have the greatest impact on the minimum group lifetime. In order to include a maximum number of vehicles into the group, more join operations have to be performed.

The presented simulations give an indication on the minimum group lifetime. In the following sections, we are evaluating the protocol for finding appropriate group lifetimes for which the obfuscation of an adversary has become high enough such that tracking is obstructed.
C. Privacy Evaluation

Our attacker model is based on an adversary, which has access to all exchanged messages within the network and is trying to reassemble the traces of observed vehicles. To resolve pseudonym changes and to track a vehicle during the group phase, a multi target tracking system based on Kalman-filter as introduced in [14] is exploited. As traceability metric we take the maximum tracking time as proposed by [7]. Assuming a group of vehicles, whose messages are observed by an adversary, we measure at which point in time a certain percentage of group members is assigned to incorrect mobility data. Simulations have been carried out with varying vehicle densities. The cell distance is set to 2600 m. For reasons of comparability we also evaluated a pseudonymization strategy based on simple pseudonym changes like the one deployed within the simTD field trial [4]. To make this approach even more effective, we reduced the pseudonym update interval to 10 seconds and assumed that all vehicles perform the pseudonym change simultaneously.

From the graph shown in Figure 13 we observe that despite the high change interval of 10 seconds and synchronization the adversary has lost very few vehicle traces only. Our experiments confirm the results obtained in [5]: A simple pseudonym change provides only a low level of privacy protection towards a global adversary.

The other three graphs in Figure 131 depict the tracking success for the proposed privacy protocol, which depends on the group lifetime. We observe a significant drop of traceability already after the first 10-20 seconds. According to our observations, higher vehicle densities are more advantageous as the likelihood for a mismatching is being increased. For the highest vehicle density of 45 vehicles/km, almost every group member becomes anonymous within the simulation timeframe of 60 seconds.

For lower vehicle densities the obfuscation for adversaries is less significant, i.e., the group has to be maintained for a longer time period to reach the same degree of anonymity for all group members. However, because the complexity for group maintenance increases over time, we are interested in a low overall group lifetime. Consequently, a trade-off between group lifetime and overall group anonymity has to be found. We argue that from simulation statistics the adversary only knows the overall tracking success in dependence of the vehicle density, but has no further knowledge upon which of his assembled traces are actually the correct ones. In the following, we assume that for most adversaries an error rate of 50 % is already high enough such that tracking is not worthwhile anymore. Under this assumption the recommended group lifetime $d_{\text{group}}$ can be determined by means of the graphs in Figure 13 as follows:

- High Vehicle Density: $d_{\text{group}} = 20$ seconds
- Medium Vehicle Density: $d_{\text{group}} = 40$ seconds
- Low Vehicle Density: $d_{\text{group}} > 60$ seconds

1 Please note that until the group has not reached a stable member size yet, the number of lost vehicles is superposed by those vehicles, which are still joining the group. Thus, in the interests of clarity, we plot the graphs starting at the Minimum Group Lifetime of 3-4 seconds (see Figure 11).
The parameters above indicate the recommended group life times for the presented motorway with a cell separation of 2600 m. These density-lifetime relations are group parameters and therefore assumed to be known by every vehicle. After group establishment a group members constantly assesses the vehicle density via its internal neighborhood table and determines how long it has to stay inside the group gain anonymity.

VII. CONCLUSION AND FUTURE WORK

In this paper we proposed and evaluated a novel approach for dynamic Mix Zones. We stated the main objectives for C2X privacy solutions and developed our approach accordingly: A major aspect of the presented protocol is the decentralized group key generation algorithm based on exchanged key fragments. Compared to centralized approaches, decentralized group establishment and maintenance reflects much more the cooperative nature of Car-to-X networks and avoids policy issues (refers to objective Decentralization). In order to make the protocol robust against message losses, we developed the concept of Member and Request Sets (refers to objective Robustness). For group maintenance several sub-protocols have been specified in order to dynamically integrate further vehicles into the group and to handle group interference with adjacent groups (refers to objective Flexibility). Evaluations on protocol timing yielded acceptable performance margins of for group establishment. The low latency is mainly achieved by piggy-bagging the key fragments with frequently sent CAMs (refers to objective Efficiency). During the group process we advocate signing messages instead of encrypting them. Certainly, encrypted messages have the advantage of reduced traceability as the message content is not readable by external adversaries. However, this also implies that CAM messages cannot be processed by adjacent trustworthy vehicles as long as they are not yet part of the group. Due to safety reasons this is not a preferable solution (refers to objective Safety-Preservation). To enable lawful interception, every message is further authenticated using a symmetric CA key (refers to objective Accountability). We modeled a powerful global adversary and evaluated the gained privacy enhancements by means of simulations. Our results show that dynamic Mix Zones provide a significantly higher unlinkability of pseudonym changes, compared simple pseudonym changes (refers to objective Privacy Enhancements).

In our future work we are analyzing the feasibility of the privacy protocol for additional road types, e.g., inner city scenarios. Furthermore, for more detailed evaluations, we are exploring how to include the proposed privacy protocol into the currently running simTD field trial.

ACKNOWLEDGEMENT

We would like to thank the DCATI institute at TU Berlin for providing the V2X Simulation Runtime Infrastructure including road maps.

REFERENCES

[1] simTD: Safe and Intelligent Mobility Test Field Germany. [Online]. www.simTD.de