An Efficient Anonymous Authenticated Key Agreement Protocol for Vehicular Ad-Hoc Networks Based on Ring Signatures and the Elliptic Curve Integrated Encryption Scheme

Carsten Büttner[1](✉) and Sorin A. Huss[2]

[1] Adam Opel AG, Advanced Technology, Rüsselsheim am Main, Germany
carsten.buettner@de.opel.com
[2] Integrated Circuits and Systems Lab,
Technische Universitt Darmstadt, Darmstadt, Germany
huss@iss.tu-darmstadt.de

Abstract. Privacy in Vehicular Ad-hoc NETworks (VANETs) is one of the most important issues in order to successfully attract users to this new technology. In a common VANET use case two vehicles using the same application frequently need to exchange confidential application-related data. When it comes to a confidential data exchange, both vehicles need to authenticate each other and to agree on an encryption key. The new protocol proposed in this paper satisfies these requirements and, in addition, preserves the privacy of the vehicles. After execution of the protocol neither any vehicle in the communication range nor even the communication partners can reveal the identity of any of the communicating vehicles. To achieve this important goal we rely on the standardized Elliptic Curve Integrated Encryption Scheme (ECIES) and on ring signatures. We demonstrate how the advocated protocol can be used within GeoNetworking messages and evaluate its characteristics regarding the privacy of the participating vehicles. The presented results clearly show that the number of necessary pseudonyms for each vehicle may be reduced considerably when compared to a sole ECIES usage while still maintaining the privacy of the vehicles.

Keywords: Anonymous authentication · Vehicular Ad-hoc NETworks · Key agreement · Ring signatures · ECIES

1 Introduction

For safety reasons vehicles in Vehicular Ad-hoc NETworks (VANETs) use broadcast over ITS-G5 to inform other vehicles in the communication range about their current status, including position, heading, and speed. All safety messages are digitally signed to prove the integrity of the message and eligibility of the

O. Camp et al. (Eds.): ICISSP 2015, CCIS 576, pp. 139–159, 2015.
DOI: 10.1007/978-3-319-27668-7_9

sender. Since every participant shall receive and interpret these messages as fast as possible, they are in general not encrypted. Besides this safety relevant communication, there are other applications available where the data exchanged between vehicles is confidential and therefore needs to be encrypted.

Consider as an example a service provider that collects data about potholes on roads in a certain area. Vehicles thus record data about potholes and report it to the service provider, which subsequently offers the data to other service providers or local administrations. However, the data sent to the service provider contains privacy related data such as the location of the pothole and a coarse time, when it was detected. If all vehicles would simply sent their detected data to the service provider, then this entity may create movement profiles of the vehicles out of the reported data. In order to preserve the privacy of its users and to advertise the privacy considerations, the service provider decides to implement a privacy preserving mechanism. This mechanism requires that the vehicles exchange their collected data between each other prior uploading. When using this mechanism the vehicles report pothole locations detected by other vehicles too. Therefore, the service provider can no longer determine where a specific vehicle was driving at the given point in time and can no longer create movement profiles of this vehicle. The provider may decide to use the ETSI ITS-G5 network to exchange the data between the vehicles, because it is free of charge. In addition, the provider enforces an encrypted data exchange policy, so no attacker can record and sell the collected data next to the service provider. The exchange of the encrypted data shall also be privacy preserving.

In general, there are three basic problems to be considered, when confidential data is being exchanged between vehicles: (i) How does a vehicle ensure whether the other vehicle is eligible to receive confidential data? (ii) How do vehicles exchange the key for encrypting their communication data? (iii) How can the first two problems be solved while preserving the privacy of the vehicles?

For safety-related communications in VANETs each vehicle uses a pseudonym to sign all messages. To ensure the privacy of the vehicle the pseudonym is changed on a regular basis, so that two pseudonyms cannot be linked to the same vehicle. Of course, a vehicle might simply use an own set of pseudonyms for each application by encoding the application into the pseudonym and exploit well-known key agreement protocols like the Elliptic Curve Integrated Encryption Scheme (ECIES) as standardized in [15] to authenticate against each other and finally to agree on an encryption key. However, the vehicle then needs to change its pseudonym for the application at hand at the same time as the one intended for safety-related communication to prevent linking of pseudonyms. This introduces a cost overhead both for additional secure storage of the private keys and for the data transmission aimed to obtain new pseudonyms. Therefore, we propose in the sequel a novel protocol that solves all three outlined problems and at the same time reduces the number of necessary pseudonyms in comparison to exploiting ECIES only. In order to do so we pick up the concept of k-anonymity [19], combine ring signatures [17] with the ECIES scheme, and evaluate the resulting protocol with respect to the privacy of the vehicles.

The rest of this paper is organized as follows: In Sect. 2 we discuss the term of application-specific pseudonyms. The state of the art of anonymous authenticated key agreement protocols is reviewed in Sect. 3. We then introduce the new anonymous authentication scheme in Sect. 4. The evaluation of this protocol is presented in Sect. 5. Finally, we conclude the paper in Sect. 6.

2 Application-Specific Pseudonyms

Each vehicle participating in a VANET is equipped with a set of certificates to sign safety messages. These certificates are named pseudonyms, since they do not leak the identity and therefore preserve the privacy of the vehicle. In this paper we assume that each application such as the outlined pothole detection service issues its own pseudonyms, thus proving that the owner of the corresponding private key is eligible to run the application. So, only vehicles equipped with a valid pseudonym can get access to it. We name such pseudonyms *application-specific pseudonyms.*

An unique identifier is assigned to each application in order to determine which pseudonym belongs to which application. In case that this identifier is also part of the pseudonym, the application can check, whether the pseudonym is eligible to use the service. Pseudonyms used in VANETs contain an ITS Application ID [11], which may be exploited for this purpose.

3 Related Work

The IEEE Standard 1609.2 for Wireless Access in Vehicular Environments [15] uses the hybrid encryption scheme ECIES to encrypt messages between vehicles. In ECIES both parties agree on a key to encrypt and exchange an AES key. This AES key is later on used to encrypt the exchanged data. However, since it is necessary that the vehicles change all their identities each time the safety pseudonym changes, one set of pseudonyms with the same size as the one for safety messages would be necessary for each single application to prevent linking pseudonyms. We reduce the considerable size of the sets necessary for each application by combining ECIES with ring signatures.

Ring signatures based on RSA and Rabin's signature scheme have been introduced in [17]. In order to create a signature, the signer takes in addition to his own private key the public key of n other entities to sign the message. To verify the message, the public key of the signer and the n public keys of the other entities are necessary. The verifier of a ring signature cannot distinguish who of the $n+1$ entities actually signed the message because the probability of each signer results in $1/(n+1)$. The authors of [16] propose ring signatures for anonymous routing in wireless ad-hoc networks, but they did not evaluate related ring building strategies nor the size of the protocol nor multiple own pseudonyms. In [14] the authors advocate ring signatures in mobile ad-hoc networks for authentication of neighbor nodes. They did investigate ring building strategies, but most of their strategies require either a central server or the nodes have to be a-priori aware of the pseudonyms of all other nodes. In addition, these authors only considered the case where each node has just one pseudonym and elaborated a general formula to calculate the transmission overhead, but they did not evaluate their suggestion.

Secret Handshakes [2,5] are used to identify secretly if two parties belong to the same group. Even if the handshake fails, both parties cannot retrieve the group of the opposite. Accordingly, a third party is never able to retrieve the affiliation of a participant to a group. To reach unlinkability between different handshakes, an unique pseudonym has to be used for each handshake. Otherwise an attacker may eventually link different handshakes to a specific participant. This method is similar to the usage of ECIES in VANETs with regular pseudonym changes. However, we aim to significantly reduce the amount of required pseudonyms compared to this method.

Group Signatures [6] allow a member of a group to create a signature on behalf of the group. The verifiers can only prove that the signature was created by a member of the group but not by whom. Unfortunately, group signatures are not suitable for the envisaged scenario, because each time a user leaves the group, new credentials have to be distributed to all group members. This property obstructs in our case the scalability of the approach because of the high probability that multiple vehicles leave the group every day. Moreover, we cannot assume that all vehicles are quipped with mobile communication devices to obtain on time the required information from the central entity.

An Anonymous Credential [4] is a set of attributes issued by a trustworthy entity. An user can prove a subset of her attributes to a verifier without revealing her identity, whereas several proofs cannot be linked. Again, Anonymous Credentials are not suitable in our case, because they require a regular connection to a central entity to get revocation information. As before, we cannot assume that all vehicles are linked to a central entity, because we cannot assume that all vehicles are equipped with a mobile communication. In addition, proofs of attributes do not establish an encryption key and show a high computational complexity.

Matchmaking Protocols [1] are intended to authenticate two members of the same group without revealing their group to others. However, this scheme does not hide the identity of the members, it hides only the group they are a member of. In contrast, we need to hide the identity of the members and not of the group.

The authors of [12] propose to use Physical Unclonable Functions (PUFs) to generate the private keys of the pseudonyms. This may well reduce the amount of necessary secure storage for the private keys of the pseudonyms. However, we aim to directly reduce the number of necessary pseudonyms. This also diminishes the amount of necessary secure storage, because less keys have to be stored, but also reduces the number of keys to be generated, of certificates to be issued by the infrastructure, and the amount of data to be transmitted to the vehicle. The advocated protocol can be used to reduce the overall number of necessary pseudonyms and, in addition, PUFs may be exploited to decrease the amount of necessary secure storage.

K-anonymity as defined in [19] provides a metric to measure the anonymity of a subject, where k denotes the number of subjects it is indistinguishable from. This metric will be exploited in the sequel for the envisaged scenario.

4 Anonymous Authentication

In this section we first specify the requirements of the proposed anonymous authenticated key agreement protocol and then present it in detail. We also characterize possible attacks and comment on the protocol parameters considered so far.

An anonymous authenticated key agreement protocol allows two parties, who are members of the same group, to establish a confidential communication. To achieve this goal, both parties have to agree on a session key to encrypt the exchanged messages. The identity of the other party is unknown at the beginning of the protocol and both parties are not willing to expose for privacy reasons their application-specific identity to anyone. In addition, it shall be possible to revoke access for single parties and only members of the same group shall be able to agree on the session key. The protocol shall fail, if one party is not a member of the group. Not eligible parties shall gain as few information as possible about the other party. We only consider single-hop connections, because multi-hop connections are difficult to maintain in VANETs due to frequent topology changes.

4.1 Protocol

The advocated key agreement protocol takes the approach proposed by the authors of this paper in [3] as a foundation and relies on both the ECIES scheme and ring signatures. Such a signature is intended to sign the transmitted ECIES parameters. By combining ECIES with ring signatures, the vehicles agree on a symmetric encryption key as standardized in [15] and bind this key to a specific application with the help of a ring signature created with application-specific pseudonyms. This generic approach has the advantage that the vehicles can use the safety identities already known to each other for ECIES and hide the application-specific identity by means of ring signatures. So, it is no longer possible to identify the entity which actually created the signature. The only information to be derived points to the set of pseudonyms present in the ring. Therefore, the application-specific pseudonyms can be reused after a pseudonym change without any link to safety pseudonyms. As a consequence, less application-specific pseudonyms are necessary. We exercise the ring signature scheme based on elliptic curves as proposed in [16]. We favor this scheme, since elliptic curves provide the same security level with a much shorter signature length compared to RSA. In addition, we propose a second version of the protocol, where the pseudonyms of the ring signature are encrypted together with the signature. We denote these protocol versions as non-encrypted and encrypted, respectively.

We introduce the following notation for the description of the protocol: *Service Announcement* denotes a service announcement according to [10]. V, C, and T are defined according to [15]: V is the public key of the sender, the parameter C is the symmetric AES key K encrypted by ECIES, while T denotes the authentication tag of ECIES. The pseudonym of entity X is denoted as $Cert_X$. The ring signature consists of n different pseudonyms $Cert_{Xn}$, where one is an application-specific pseudonym of the respective signer and the others are the collected application-specific pseudonyms. The values x_{Xn} are necessary to validate the ring signature. The actual ring signature is denoted as σ. When Y is encrypted with the encryption key K, it is denoted as $E_K(Y)$.

The non-encrypted version of the protocol is defined as follows and is discussed in the sequel.

(1) A → *: $ServiceAnnouncement$
(2) B → A: $V, C, T, Cert_{B1}, ..., Cert_{Bn}, x_{B1}, ..., x_{Bn}, E_K(\sigma)$
(3) A → B: $Cert_{A1}, ..., Cert_{An}, x_{A1}, ..., x_{An}, E_K(\sigma)$

In Step 1 Alice (A) announces that she offers a service that uses the anonymous authenticated key agreement protocol.

Assuming Bob (B) receives the service announcement from Alice and wants to use this service, he first generates an AES key K as payload for ECIES and calculates V, C, and T according to the ECIES scheme. Then he selects $n-1$ pseudonyms from his collected pool and one of his own pseudonyms in order to calculate the ring signature σ over V, C, and T. Then, he encrypts σ with the symmetric key K. Finally, he sends V, C, T, the ring signature, and everything necessary for validation to Alice (Step 2).

After reception Alice decrypts the AES key K according to the ECIES scheme and applies it to decrypt σ before validating the ring signature. In case that the validation was successful, she selects both one of her own pseudonyms and $n-1$ collected pseudonyms. With this set of pseudonyms she calculates a ring signature σ over V, C, and T and encrypts it with K. Then she sends the ring signature and everything necessary to validate it to Bob (Step 3).

When Bob receives the ring signature from Alice, he decrypts σ and validates the ring signature. If the validation was successful, he starts the confidential communication with Alice. After the execution of the protocol, Alice and Bob know that the other party is authorized to use the service. In addition, both are in possession of the same encryption key K still without knowing the application-specific identity of the other party.

The encrypted version of the protocol differs in Steps 2 and 3. The difference to the non-encrypted one is that not only σ is encrypted, but additionally all necessary data to validate the ring signature. This version is defined as follows.

($2^{'}$) B → A: $V, C, T, E_K(Cert_{B1}, ..., Cert_{Bn}, x_{B1}, ..., x_{Bn}, \sigma)$
($3^{'}$) A → B: $E_K(Cert_{A1}, ..., Cert_{An}, x_{A1}, ..., x_{An}, \sigma)$

Given that the other party and a potential attacker already know the pseudonym used for safety messages, the identity applied to execute the ECIES scheme does not give an attacker any new knowledge. These safety pseudonyms should be changed on a regular basis and not be reused. Therefore, they cannot be exploited to track anything. The goal of an attacker is to determine the application-specific pseudonym of a vehicle, since this will be reused in different ring signatures and may therefore be used to link different safety identities of the vehicles. This may be achieved, when a vehicle exploits the same application-specific pseudonym twice, but with different pseudonyms for safety communication in VANETs. Then, an attacker can link the two safety pseudonyms, because they are used in combination with the same application-specific pseudonym.

Thus, please consider the case that Alice applies the safety pseudonym $Cert_{S1}$ and application-specific pseudonym $Cert_{A1}$ at the same time. Then, she changes her safety pseudonym to $Cert_{S2}$, while still using the application-specific pseudonym $Cert_{A1}$. An attacker now may link $Cert_{S1}$ and $Cert_{S2}$ because they were exploited with the same application-specific pseudonym.

We assume that each vehicle may have multiple valid application-specific pseudonyms at a time. So, the vehicles are in the position to change their application-specific pseudonym they use for building the ring signature regularly with their pseudonyms for safety relevant communication to avoid being tracked by means of the pseudonyms not being changed.

Multiple pseudonyms confuse an attacker considerably, since each vehicle features multiple identities and these identities may easily be used at the same time in ring signatures of different vehicles. We evaluate the impact of multiple parallel pseudonyms in Sect. 5.

For the outlined protocol we stick for compatibility purposes to the same pseudonym format already existing in VANETs to sign safety messages, however we bind them to a specific application. We also exploit elliptic curve cryptography and ECIES, which is already standardized for safety communication. Therefore, this protocol fits very well in the present VANET environment.

It is quite simple to exclude a vehicle from successfully executing the protocol by revoking its application-specific pseudonyms. The revocation may be done in the same way as for safety pseudonyms.

4.2 Message Format

To address the receiving vehicle, the actual protocol payload needs to be encapsulated in a network protocol. Due to the high mobility in VANETs, GeoNetworking [7] is used to address the receivers of a message. When using GeoNetworking, the vehicles define an area wherein the message is relevant and the message is then distributed within this area. For safety applications the receiver is not a single vehicle, but all vehicles in the destination area. However, it is also possible to address a single vehicle as the receiver of a message. Due to the ad-hoc characteristics of the network even in this case the geographic region of the vehicle is necessary too. In order to address a single vehicle, it needs a so called GeoNetworking address.

GeoMessaging messages are structured according to [7] as follows. They always start with a Basic Header for general information followed by a Secured Package. The Secured Package contains all immutable content of the message and can be split into Header Fields, Payload Fields, and Trailer Fields. The

Header Fields contain security related information. The Payload Fields can be separated into a Common Header for general immutable content, an Extended Header for the definition of the origin and destination, and the actual payload of the message. The Extended Header can be for example a Geographically-Scoped Broadcast (GBC) packet header to address all vehicles in a geographic region or a Geographically-Scoped Unicast (GUC) packet header to address a single vehicle. The Trailer Fields contain basically a signature over the complete secured packet. The structure of the GeoNetworking message is depicted in Fig. 1.

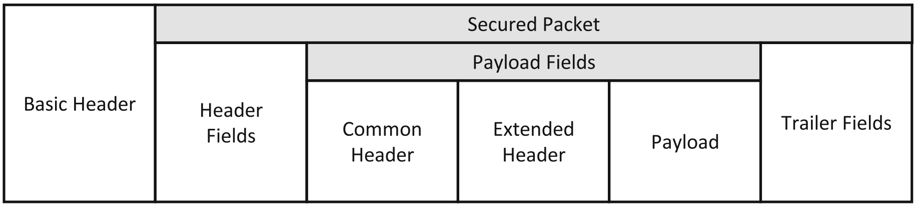

Fig. 1. GeoNetworking message format.

For the proposed protocol GUC messages are most suitable, because the exchanged messages are only relevant for a single receiving vehicle. Therefore the Extended Header will be a GUC packet header. The format of the service announcement message (Step 1) is sent via broadcast to all vehicles in proximity and already standardized in [10]. Due to this reason, we will discuss in the sequel the used format only for the subsequent messages.

The Basic Header consists of a version number, the type of the next header (Secured Package), the remaining lifetime of the message, and the remaining hop limit. The contents of the Header Fields are defined by profiles. A profile defines the header fields to be included from a list of all possible fields. The corresponding standard [11] defines a generic profile, one for CAM messages, and one for DENM messages. However, none of these profiles are suitable for the advocated protocol. Therefore, we defined a dedicated profile. It consists of the generation time of the message aimed to detect replay attacks and a signer info, which is the pseudonym for safety relevant communication of the sender to check the authenticity of the message. This profile is used for all messages of the outlined protocol. The encrypted messages exchanged subsequently can use this profile too. The Common Header defines the next header (in our case the GUC-Header), the traffic class of the message, the length of the payload, the maximum hop limit, and whether the station is mobile or not. The GUC package header is responsible for the addressing of the recipient and contains a sequence number, information about the source like its GeoNetworking address and position, and the GeoNetworking address, position and timestamp of the last known position of the receiver. The payload is the data denoted in the protocol Steps 2 and 3, respectively. The Trailer Fields contain a signature over the content of the Secured Package

The overhead introduced by GeoNetworking is considered in the evaluation of the message size of the protocol in Sect. 5.1.

4.3 Attacker

Capabilities. We distinguish between *passive* and *active attackers*. A passive attacker can only listen to and record exchanged messages, while active attackers can also replay and send messages under a forged identity. We consider four types of active attackers that differ in their access to pseudonyms as detailed in Table 1. The least powerful attacker has no access to any valid pseudonyms. Another attacker has only access to pseudonyms for safety relevant communication. The third one has only access to application-specific pseudonyms, while the most powerful attacker is an insider and has access to both pseudonym types.

Table 1 compares the encrypted and non-encrypted version of the protocol regarding the information the different attacker types can yield. We consider the size of the ring and the pseudonyms used by Alice and Bob as critical. When the attacker can get the respective information, it is denoted as X, otherwise as O.

Table 1. Capabilities of attackers.

Attacker	Protocol	Ring size	Alice	Bob
Passive	Non-Encrypted	X	X	X
	Encrypted	X	O	O
Active without pseudonyms	Non-Encrypted	X	X	X
	Encrypted	X	O	O
Active with safety pseudonyms	Non-Encrypted	X	X	X
	Encrypted	X	O	X
Active with application pseudonyms	Non-Encrypted	X	X	X
	Encrypted	X	O	O
Active with safety and application pseudonyms	Non-Encrypted	X	X	X
	Encrypted	X	X	X

Regardless of the used version of the protocol, all attackers can calculate the current ring size from the message size. When the non-encrypted version is used, all attackers can get the pseudonyms used by Alice and Bob, since they are transmitted in plain text. Therefore, only the capabilities of the attackers regarding the encrypted version of the protocol are discussed in the sequel.

The passive attacker cannot get the pseudonyms of Alice and Bob when the encrypted version is used, since they are encrypted and the attacker cannot derive the encryption key K just by listening to the exchanged messages.

Without access to valid pseudonyms, an active attacker is not able to successfully inject any message, since all of them are either signed or encrypted. If the attacker replays the first message, she cannot encrypt the second or reply a valid third message, since she does not know and cannot calculate the encryption key. If she replays the second message, she is not in the position to decrypt the pseudonyms used by Bob in Step 3, since she does not know and cannot calculate the encryption key. Therefore, all active attackers are not able to get any information by replaying messages.

An active attacker with access to pseudonyms for safety relevant communication may generate and send the first messages. If she sends the first message, she cannot replay with the third step, because she has no application-specific pseudonym available in order to generate a valid ring signature. However, she can decrypt the pseudonyms used by Alice in Step 2 by calculating the encryption key K and therefore can get the pseudonyms used by Alice. The attacker is also not able to generate a valid second message, since a valid application-specific pseudonym is necessary for this purpose.

An active attacker, who has only access to application-specific pseudonyms, cannot generate and send a valid service announcement, because it is signed with a pseudonym for safety relevant communication. The same holds for the second message.

If an active attacker has access to both a pseudonym for safety relevant communications and to an application-specific pseudonym, she is now in the position to send and to answer to all messages of the protocol and therefore gets the pseudonyms used by Alice and Bob.

This analysis shows, that only the most powerful active attacker is able to unveil the identities used by Alice and Bob when the encrypted version of the protocol is being applied. However, lots of sophisticated work will be necessary to implement this type of attacker in practice, since the private keys of the pseudonyms are in general stored on a hardware security module (HSM) inside the vehicle. Of course, if the HSM fails and an attacker is thus able to extract the private keys, she can get both the valid safety and the application-specific pseudonyms and send valid fake messages. However, then the attacker may also extract only the private keys of the safety pseudonyms and link them directly or send valid fake safety messages. In general, it is possible to detect and to revoke the affected vehicle, which works well with the proposed protocol. However, failed HSMs are a general problem in VANETs and we will therefore not address it in more detail in this paper.

Behavior. In this section we discuss the behavior of the considered attacker. This attacker is a passive one aiming at the non-encrypted version of the protocol. This attacker type is sufficient, because even the most powerful attacker aiming at the encrypted version cannot gain more information. The attacker tries to identify the application-specific pseudonym of a vehicle from the ones used in the ring signature. The behavior of the attacker can be characterized by three stages.

```
// Count pseudonym usage
Create hashmap $hm$ for pseudonym usage
**for** each colected message $m$ **do**
    **for** each used pseudonym $p$ in $m$ **do**
        **if** $hm.contains(p)$ **then**
            $hm.put(p, hm.get(p) + 1)$
        **else**
            $hm.put(p, 1)$
        **end if**
    **end for**
**end for**
// Select relevant pseudonyms
Create list $relevantPseudonyms$
**for** each pseudonym $p$ in $hm$ **do**
    **if** $p > DaysObserving/PseudonymPoolSize$ **then**
        $relevantPseudonyms.add(p)$
    **end if**
**end for**
```

Fig. 2. Pseudonym filtering algorithm used by the passive attacker.

In the first stage the attacker just records the exchanged messages.

After recording, the attacker counts how often each pseudonym has been applied. Then, she selects the relevant pseudonyms, which are used at least $DaysObserving/PseudonymPoolSize$ times, where $DaysObserving$ denotes the number of days the attacker recorded the messages and $PseudonymPoolSize$ the number of own pseudonyms each vehicle has at the same time, respectively. Thus, only pseudonyms used regularly are considered. The filtered ones might be introduced to the communication by vehicles driving only once the observed street. The pseudocode for this second stage is shown in Fig. 2.

The the third and last stage starts with the identification of unambiguous pseudonyms and is shown as pseudocode in Fig. 3. A pseudonym is unambiguous, if it is the only relevant pseudonym of a ring. Therefore, this pseudonym must be the identity of the vehicle. Afterwards, these unambiguous pseudonyms are deleted from all rings of the other vehicles on this day. By 'delete' we mean that it is now clear that this pseudonym does not belong to the vehicle and we therefore do no longer need to consider it in the respective rings.

If each vehicle applies an own ring size, unambiguous pseudonyms are also deleted from the vehicles using a different ring size in other days. By 'own ring size' we mean that not all vehicles use the same number of pseudonyms to construct their ring signature. We may delete these pseudonyms, because we know the ring size of the vehicle owning the pseudonym is different.

If any pseudonyms were deleted, the attacker tries to identify new unambiguous pseudonyms, otherwise the attacker is finished. Now the attacker has reduced the ring size of the vehicles by excluding pseudonyms, which cannot be the identities of the vehicles. We evaluate in Sect. 5.2 by how much the attacker

```
do
    $reduced = false$
    // Identify unambiguous pseudonyms
    Create list $unambiguousPseudonyms$
    for each collected message $m$ do
        for each pseudonym $p$ in $m$ do
            if $m.relevantPseudonyms == 1$ then
                $unambiguousPseudonyms.add(p)$
            end if
        end for
    end for
    // Reduce ring sizes
    for each collected message $m$ do
        for each pseudonym $p$ in $m$ do
            if $p \in unambiguousPseudonyms \wedge$
            $m.day == unambiguousPseudonyms.get(p).day$ then
                m.delete(p)
                $reduced = true$
            end if
        end for
    end for
    // Handle different ring sizes
    if $differentRingSizes$ then
        for each collected message $m$ do
            for each pseudonym $p$ in $m$ do
                if $p \in unambiguousPseudonyms \wedge p.ringSize! = m.ringSize$ then
                    m.delete(p)
                    $reduced = true$
                end if
            end for
        end for
    end if
while $reduced == true$
```

Fig. 3. Ring size reduction algorithm used by the passive attacker.

can reduce the ring size and therefore the k-anonymity value in presence of various parameters.

4.4 Considered Parameters

The anonymity of the vehicles is influenced by various parameters when they use the proposed anonymous authentication protocol. We considered the following parameters in the subsequent simulation runs.

Ring Size: The number of pseudonyms present in the ring signature. Unless explicitly mentioned, we used the maximum possible ring size of 10 according to Fig. 4.

Fraction of One Time Vehicles: These vehicles use a set of pseudonyms in their ring that is completely unknown to the other vehicles. They shall reflect that most vehicles drive the same route each day, but there are always vehicles that normally do not take this route in rush-hour, e.g., trucks. Unless explicitly mentioned, we consider 30 % of such one time vehicles.

Standard Deviation of the Starting Times: The starting times of the vehicles are assumed to be normally distributed. The standard deviation has an influence on the potential communication partners. Unless explicitly stated we use a standard deviation of 5 min.

Ring Building Strategy: When ring signatures are in place, a vehicle is one of n possible signers. It is important to apply a good ring building strategy, because a poor strategy can lead to revealing of most or even all of the non-signers, so the anonymity of the signer may decrease significantly. In the following we propose some appropriate strategies to build a ring. We evaluate these strategies later on in Sect. 5.

All: The vehicles collect and save all pseudonyms they receive from other vehicles. When the vehicles need to build a new ring, they randomly select the required number of pseudonyms from their pools.

SameDirection: Vehicles using this strategy collect and save all pseudonyms they receive from other vehicles driving in the same direction. The basic idea behind this method is that vehicles in rush-hour drive every day at approximately the same time in the same direction. Therefore, an attacker cannot delete the pseudonyms of the vehicles driving each day in the opposite direction from the ring. The same ring building method as for “All” is applied.

SameDirectionLastX: This strategy is similar to “SameDirection”. The main difference is that the vehicles discard pseudonyms they met more than X days ago. The reason for this is that each day the vehicles collect pseudonyms of one time vehicles they never met before and unlikely meet again. If a vehicle uses such pseudonyms in its ring, an attacker can identify and remove them to get the identity of the victim vehicle. This can be done because they are less used than other pseudonyms. When limiting the number of pseudonyms by the number of previous days, the influence of these vehicles decreases. Unless explicitly mentioned, we use this ring building strategy.

SameDirectionLastXDifferentSizes: This strategy works like “SameDirection-LastX”, but each vehicle applies an own ring size. This strategy is evaluated later on to assess the influence of different ring sizes on the anonymity of the vehicles.

Number of Own Pseudonyms: The number of own pseudonyms a vehicle has at the same time. Each time a ring is being build, the vehicle randomly selects one. Unless explicitly stated, we exploit 10 simultaneous pseudonyms.

Duration of the Attack: The duration denotes the number of days the attacker listens to the exchanged messages. Unless explicitly mentioned, we consider an attack duration of 30 days.

Number of Previous Days: This parameter denotes the number of days a vehicle stores the collected pseudonyms in the strategies *SameDirectionLastX* and *SameDirectionLastXDifferentSizes*.

5 Evaluation

5.1 Ring Size

The ring size denotes the number of pseudonyms used in the ring signature. It is obvious that the k-anonymity of the vehicle increases with the ring size. Since we want the maximum possible anonymity for the vehicles, we try to make the ring as large as possible, but we also have to avoid at the same time any fragmentation at the MAC layer [8].

To determine the maximum feasible message size, we measured the size of the largest message in the protocol. In this implementation we exploited the elliptic curve ring signature scheme proposed in [16] with curve P-256 and ECIES as described in [15]. For the pseudonym size we took 161 bytes, which is the size of a pseudonym certificate of the Pilot PKI of the Car-2-Car Communication Consortium[1]. We also took advantage of elliptic curve point compression [20] to minimize the size of the messages.

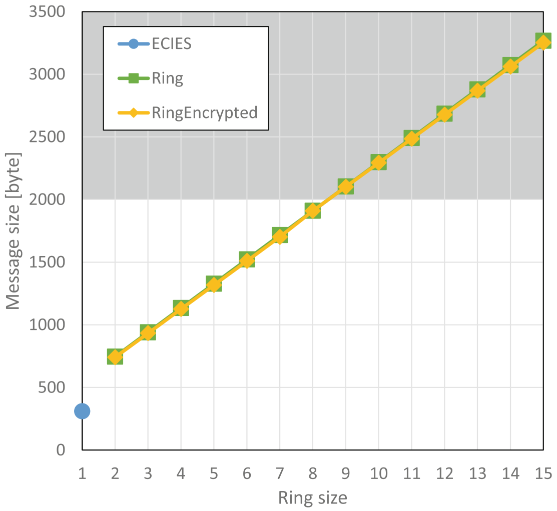

Fig. 4. Size of the largest message as a function of ring size: Size of largest message.

The size of the largest message as a function of the ring sizes as well as for ECIES without ring signatures is shown in Fig. 4. The darker area indicates the

[1] www.car-2-car.org.

Maximum Transmission Unit (MTU), which is expected to be larger than 2.000 bytes [9]. ECIES without the ring signatures has the lowest message size at an anonymity of 1. For ring signatures the message size increases linearly with the ring size. Due to the fixed size of the secured GeoNetworking packet headers and trailers (240 bytes), V (33 bytes), C (16 bytes), and T (20 bytes) the size of the message increases with every ring member by the size of a $Cert$ (161 bytes) and an x (32 bytes), which are in total 193 bytes. The graph indicates that depending on the MTU ring signatures with 9 or more members are the ones with the maximum anonymity in VANETs, when fragmentation at the MAC layer shall be avoided. We demonstrate in the following that a ring signature with 10 members is sufficient for the protocol and use case presented in order to preserve the privacy of the vehicles while reducing the number of necessary pseudonyms.

Messages of this size are much larger than safety messages. However, they are sent at a much lower frequency: Safety messages are sent up to 10 times a second, whereas the messages in the proposed protocol for the envisaged use case will be sent only a few times per hour. The messages are also sent on a different channel as the safety messages and do not have critical time constraints like safety messages. The envisaged channel is expected to be also used for Internet browsing, video streaming, or software updates.

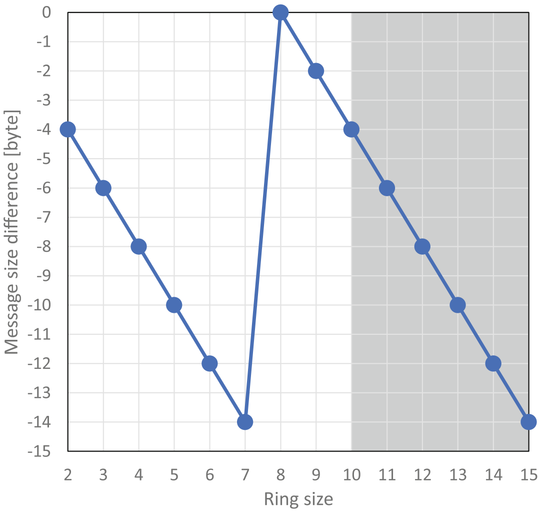

Fig. 5. Message size as a function of ring size: Size difference of encrypted and plain message.

Figure 5 shows the difference of the largest message of the encrypted and non-encrypted version in bytes. The negative values indicate that the encrypted version of the protocol has a smaller message size. When the non-encrypted version is applied only the signature is encrypted. It has a length of 33 byte and is therefore stored in three AES blocks of 16 bytes each, where the last block is padded with 15 bytes. In the encrypted version of the protocol more data is encrypted, whereby less padding bytes are used and therefore the overall message size is reduced. The darker area indicates the ring size when the MTU is in operation.

5.2 Simulation

Setup. For we exploited the VSimRTI tool set [18]. As simulation scenario we selected the motorway A60 south of Rüsselsheim, Germany. At each junction of the motorway one RSU is placed, which is assumed to be under control of an attacker, who can record all messages exchanged in the communication range. The vehicles enter the simulation area at two points: One in the east for the vehicles driving westbound and one in the west of the map for vehicles driving eastbound.

Normally the same vehicles drive the same way every day during rush-hour. Because these are ideal conditions for an attacker to link pseudonyms used at different days, we evaluated the privacy protocol under this condition. According to the traffic density categorization in [13] we applied a high density of vehicles in one and a low density in the other direction. Three classes of vehicles are considered in the simulation: The fast ones have a maximum speed of 130 km/h, the regular ones a maximum speed of 110 km/h, and the slow ones of 80 km/h. The different vehicle classes are equally distributed. The vehicles only drive the maximum speed if the traffic conditions allow it. They also overtake only if there is space to do so. Ten percent of the vehicles are equipped with an application software that uses the proposed anonymous key agreement protocol.

The envisaged simulation duration is 60 min. Since it takes some time until the simulation is adjusted, we cut 10 min both at the beginning and at the end of the simulation. Due to the long simulation duration, we decided to run the simulation without a specific ring building strategy. Instead, we log which vehicles establish a session key to map the ring building strategies afterwards on the vehicles. To evaluate more than 50 days, we randomly select as much simulation results as necessary from the pool of all 50 simulation runs and map the recurring vehicles afterwards into the simulation results.

The elaborated results show that every day each vehicle executes the protocol at least once in the communication range of each RSU. Thus, an attacker needs only one RSU under her control to get the rings of all passing vehicles. The attacker would also not get any benefit by having control over some of the vehicles, because it is not possible to get more information in this way.

Influence of the Considered Parameters

Ring Size: The k-anonymity of the vehicles, calculated according to [19], increases linearly with the ring size from 7.0, when a ring size of 10 is used, up to 10.3 when a ring size of 15 is being considered.

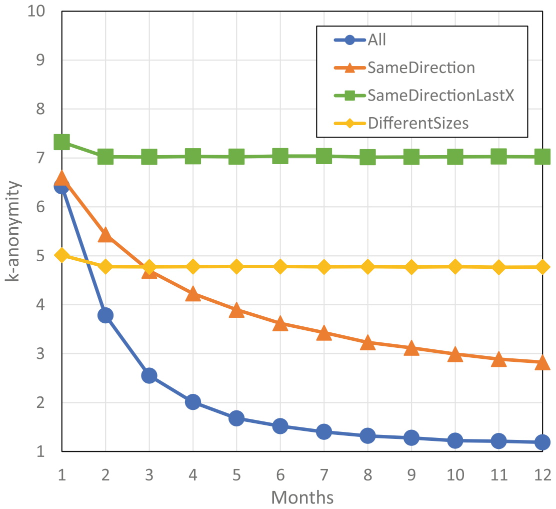

Fig. 6. Impact of ring building strategies.

Fraction of One Time Vehicles: The k-anonymity of the vehicle increases from 4.7, when 55 % of the vehicles are one time vehicles, up to 8.6, when only 11 % of the vehicles in the simulation appear only once. The reason for this is that there are more new pseudonyms in the simulations, which are considered by the vehicles during ring building.

Standard Deviation of the Starting Times: An increase or decrease of the standard deviation of the starting times had no notable influence on the anonymity of the vehicles.

Ring Building Strategy: The influence of the ring building strategy to the k-anonymity is shown in Fig. 6. The x-axis displays the month in which the attacker analyzes the messages since the start of pseudonyms usage. Month 1 is therefore the analysis of the first month and so on.

The k-anonymity value decreases over time from 6.4 in the first month down to 1.2 in the twelfth month, when the strategy “All” is in operation. The average k-anonymity value when using the “SameDirection” strategy is 6.6 in the first month and steadily decreases over time down to 2.8 after twelve months. When using the “SameDirectionLastX” strategy, the vehicles have a constant k-anonymity of 7.0 from the second month on. For the strategy “SameDirection-LastXDifferentSizes” the k-anonymity value drops from 7.0 to 4.8 compared to the case when the same sizes are used after the first month.

These results show that all vehicles should use the same ring size to keep the k-anonymity at a high level. If only pseudonyms received in the last X days are considered, then the k-anonymity of the vehicles does not decrease over time.

Number of Previous Days: To get the optimal number of previous days, we ran simulations with different day values for the various pseudonym pool sizes.

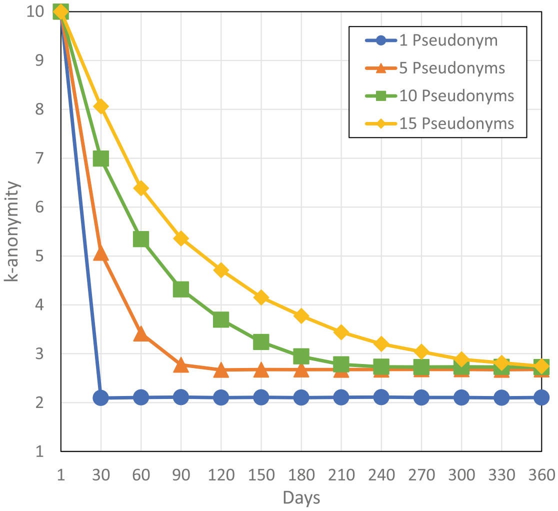

Fig. 7. Impact of pseudonym pool size.

Based on the outcome of these runs, we selected the most appropriate numbers of days.

Number of Own Pseudonyms and Duration of the Attack: Figure 7 illustrates the average k-anonymity of the vehicles for different numbers of own pseudonyms as a function of the number of days an attacker records the exchanged messages. It shows that the k-anonymity value decreases with the number of days an attacker listens to the exchanged messages. In addition, the k-anonymity value increases with the number of own pseudonyms. Depending on the assumed attack duration, either more pseudonyms have to be used or the pseudonyms have to be renewed more often in order to maintain a certain level of anonymity.

If an service provider aims to, for example, at an average k-anonymity of at least 5 for its users, the vehicles might use a new set of 5 pseudonyms every 30 days, a set of 10 pseudonyms every 60 days or a set of 15 pseudonyms every 90 days. This sums up to 60 pseudonyms per year. If we compare this value to the safety pseudonyms, where the pseudonym is to be changed at least with every trip, we can easily see that the proposed protocol reduces the number of necessary pseudonyms considerably.

A higher average anonymity of the vehicle increases the individual anonymity of the vehicles too. However, some vehicles might be still identifiable. Figure 8 visualizes the number of vehicles featuring at least a certain k-anonymity value in the case of using the same set of pseudonyms for 90 days.

The average k-anonymity for vehicles using 5 parallel pseudonyms is 2.8 for 90 days of usage (see Fig. 7). When using this setup, 16 % of all vehicles are identifiable as visible from Fig. 8. Only 9 % of the vehicles are indistinguishable

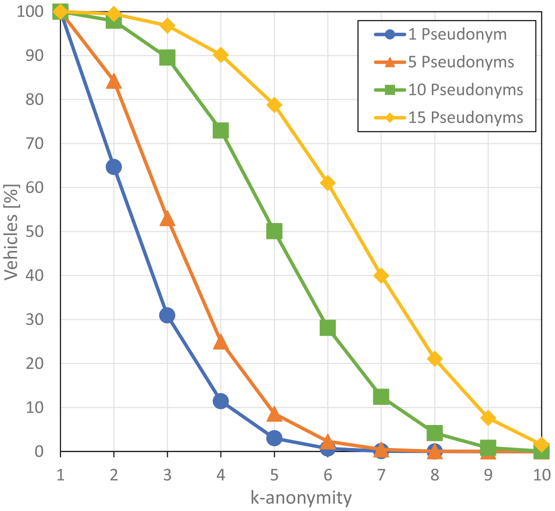

Fig. 8. K-anonymity for various pseudonym pool sizes after 90 days of usage.

from 5 or more identities. For 15 parallel pseudonyms the average k-anonymity is 5.4. Only 0.5 % of all vehicles are now identifiable while 79 % of the vehicles are indistinguishable from 5 or more identities.

6 Conclusion

In this work we proposed a novel anonymous authenticated key agreement protocol which combines ECIES with ring signatures. Based on this protocol we elaborated recommendations for an appropriate ring size for the communication between vehicles in a VANET.

We showed how the protocol can work with the standardized GeoNetworking messages aimed to address vehicles.

We demonstrated that the anonymity of the vehicles increases significantly when a good ring building strategy is applied. We also outlined that the number of pseudonyms each vehicle uses at the same time and the duration of the attack do have a clear influence on the anonymity level of the vehicles. In comparison to safety-related communication less pseudonyms for each vehicle over time are necessary to maintain a high level of anonymity, because they can be reused without the risk of being linked by an attacker. Therefore, the amount of pseudonyms, which have to be assigned to the vehicles, is significantly reduced. This both saves storage space and communication overhead and thus helps to reduce costs.

The proposed protocol is not restricted to VANET use cases, but it is especially well-suited for VANETs, because in such a context it is both expensive and some times rather difficult to obtain new pseudonyms. In addition, the well-known pseudonyms for safety-related communication can be reused by binding them to specific applications.

In the next future we plan to implement the outlined protocol into real vehicles and to take measurements to validate the presented simulation results.

Acknowledgement. This work was funded within the project CONVERGE by the German Federal Ministries of Education and Research as well as Economic Affairs and Energy.

References

1. Baldwin, R., Gramlich, W.: Cryptographic protocol for trustable match making. In: Proceedings of the IEEE Symposium on Security and Privacy (1985)
2. Balfanz, D., Durfee, G., Shankar, N., Smetters, D., Staddon, J., Wong, H.C.: Secret handshakes from pairing-based key agreements. In: Proceedings of the Symposium on Security and Privacy (2003)
3. Büttner, C., Huss, S.A.: A novel anonymous authenticated key agreement protocol for vehicular ad hoc networks. In: Proceedings of the 1st International Conference on Information Systems Security and Privacy, ICISSP (2015)
4. Camenisch, J.L., Lysyanskaya, A.: An efficient system for non-transferable anonymous credentials with optional anonymity revocation. In: Pfitzmann, B. (ed.) EUROCRYPT 2001. LNCS, vol. 2045, pp. 93–118. Springer, Heidelberg (2001)
5. Castelluccia, C., Jarecki, S., Tsudik, G.: Secret handshakes from CA-oblivious encryption. In: Lee, P.J. (ed.) ASIACRYPT 2004. LNCS, vol. 3329, pp. 293–307. Springer, Heidelberg (2004)
6. Chaum, D., van Heyst, E.: Group signatures. In: Davies, D.W. (ed.) EUROCRYPT 1991. LNCS, vol. 547, pp. 257–265. Springer, Heidelberg (1991)
7. ETSI EN 302 636-4-1: 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 (2013)
8. ETSI ES 202 663: Intelligent Transport Systems (ITS); European profile standard for the physical and medium access control layer of Intelligent Transport Systems operating in the 5 GHz frequency band (2009)
9. ETSI TS 102 636-6-1: Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 6: Internet Integration; Sub-part 1: Transmission of IPv6 Packets over GeoNetworking Protocols (2011)
10. ETSI TS 102 890–2: Intelligent Transport Systems (ITS); Facilities Layer Function, Part 2: Services Announcement (2010)
11. ETSI TS 103 097: Intelligent Transport Systems (ITS); Security; Security header and certificate formats (2013)
12. Feiri, M., Petit, J., Kargl, F.: Efficient and secure storage of private keys for pseudonymous vehicular communication. In: Proceedings of the 2013 ACM Workshop on Security, Privacy and Dependability for Cyber Vehicles, CyCAR 2013 (2013)
13. Forschungsgesellschaft für Straßen- und Verkehrswesen: Handbuch für die Bemessung von Straßenverkehrsanlagen (HBS) (2005)

14. Freudiger, J., Raya, M., Hubaux, J.-P.: Self-organized anonymous authentication in mobile ad hoc networks. In: Chen, Y., Dimitriou, T.D., Zhou, J. (eds.) SecureComm 2009. LNICST, vol. 19, pp. 350–372. Springer, Heidelberg (2009)
15. IEEE 1609.2: Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages, IEEE Standard 1609.2 (2013)
16. Lin, X., Lu, R., Zhu, H., Ho, P.H., Shen, X., Cao, Z.: ASRPAKE: an anonymous secure routing protocol with authenticated key exchange for wireless ad hoc networks. In: Proceedings of the IEEE International Conference on Communications, ICC. IEEE (2007)
17. Rivest, R.L., Shamir, A., Tauman, Y.: How to leak a secret. In: Boyd, C. (ed.) ASIACRYPT 2001. LNCS, vol. 2248, p. 552. Springer, Heidelberg (2001)
18. Schünemann, B.: V2X simulation runtime infrastructure VSimRTI: an assessment tool to design smart traffic management systems. Comput. Netw. **55**, 3189–3198 (2011)
19. Sweeney, L.: k-anonymity: a model for protecting privacy. Int. J. Uncertainty Fuzziness Knowl. Based Syst. **10**, 557–570 (2002)
20. Vanstone, S.A., Mullin, R.C., Agnew, G.B.: Elliptic curve encryption systems. Patent, US 6141420 (2000)