CoPRA: Conditional Pseudonym Resolution Algorithm in VANETs

Norbert Bißmeyer
Fraunhofer Institute for
Secure Information Technology (SIT)
Mobile Networks
Darmstadt, Germany
norbert.bissmeyer@sit.fraunhofer.de

Jonathan Petit
University of Twente
Distributed and Embedded
Security Group
Twente, Netherlands
j.petit@utwente.nl

Kpatcha M. Bayarou
Fraunhofer Institute for
Secure Information Technology (SIT)
Mobile Networks
Darmstadt, Germany
kpatcha.bayarou@sit.fraunhofer.de

***Abstract*—Wireless communication between vehicles is protected by digital certificates but these certificates and related identifiers must not be usable to track vehicles. Therefore, short-term pseudonymous certificates are applied and regularly changed in order to protect the driver's privacy. But in well defined situations, e.g. network attacks or traffic accidents, it should be possible to retrieve the appropriate long-term identifier from the certificate issuer. Hence, the resolution of pseudonym identifiers is a balancing act between full privacy and uncontrolled access to long-term identifiers.**

We propose a generic pseudonym resolution protocol that can be applied by network infrastructure entities to request pseudonym resolution information only under defined conditions. It is shown that the protocol is balanced and flexible to be applied for different use cases (e.g. lawful interception or misbehavior detection). In contrast to related protocols our solution does not increase pseudonym certificate size and avoids additional overhead and delay in the certificate acquisition phase. Further, a new feature is proposed that enables the infrastructure entities to validate the stated reason for the desired pseudonym resolution before respective information is provided. Measurements from field operational test implementations show the feasibility and practicability of the protocol when applying misbehavior detection in wireless vehicular communication networks.

I. Introduction

Communication in a wireless Vehicular Ad-hoc Network (VANET) is mainly based on messages (i.e. Cooperative Awareness Message (CAM) [1] or Basic Safety Message (BSM) [2]) that are exchanged between vehicles or between vehicles and roadside stations. This kind of communication aims to enhance future road safety and efficiency by transmitting traffic related information over a wireless IEEE 802.11p channel between aforementioned stations of an Intelligent Transportation System (ITS). As the access to this wireless channel cannot be protected physically, security mechanisms are necessary in order to establish trust between senders and receivers. The Digital Signature Standard (DSS), using public key cryptography, is a widely accepted solution for establishing message sender authentication and message data integrity and confidentiality. This cryptographic solution bases on a key pair (SK, PK) where the private key SK is handled as a secret of the owner, and the public key PK is signed by a trusted third party (i.e. Certificate Authority, CA) and distributed as a certificate to the ITS station. This security solution is also adopted and used in IEEE [3] and ETSI [4] standards for ITS security.

The location privacy of drivers should be protected by using pseudonymous identifiers in messages that may change frequently to avoid linking of recorded identifiers. According to [5], a pseudonym is an identifier that is used by a subject instead of one of its real names. Due to privacy protection requirements initially unlinked short-term pseudonyms are required in ITS communications. It should not be possible to link these pseudonymous identifiers to their long-term identifier, neither by other vehicles nor by a single trusted third party. But in defined situations, conditional pseudonym resolution may be required due to different specific circumstances as motivated in the following examples. On the one hand, a Law Enforcement Agency (LEA) may need to get long-term vehicle information based on their initially non-public pseudonyms in order to identify involved drivers in case of a traffic accident. On the other hand, a Misbehavior Evaluation Authority (MEA), that analyses suspicious communication in the VANET, may only need to know whether messages with different pseudonymous identifiers belong to the same vehicle. The task of a MEA is to identify attackers in the network by analyzing misbehavior reports that state non-plausible behavior of vehicles as further detailed in [6], [7] and [8].

In order to fulfill the aforementioned requirements regarding linkability of pseudonyms, we propose a Conditional Pseudonym Resolution Algorithm (CoPRA) that can be integrated into a Public Key Infrastructure (PKI). Using this protocol, pseudonym resolution information can be requested based on defined conditions, i.e. permissions and policies. Depending on the desired resolution information type, several independent authorities are involved in the process in order to avoid misuse. In addition, CoPRA does not decrease the performance and overhead in the vehicular wireless communication as the size of certificates and therefore the message size remains untouched. Our measurements show further that complexity and workload for the pseudonym issuance is not increased. Due to possibly instable communication links and short connection time slots between vehicles and the PKI server, the process of requesting pseudonym certificates can be realized packet-oriented rather than based on complex sessions. Further, we

focus in this paper on the specific requirements of a VANET (i.e. high speed, delay-sensitive application, high impact in case of misbehavior and strict privacy requirements). Other related network types (e.g. tactical or private MANETs and wireless sensor networks) do not generally have this specific set of requirements.

The paper is organized as follows. The CoPRA protocol is detailed in Section IV using the system model discussed in Section III. We analyze its adequacy for ITS communication in Section V and show the applicability for misbehavior detection in Section VI. We also compare it with other related protocols by means of performance and overhead. A detailed performance measurement is further presented in Section VI-C whereby CoPRA is implemented in the public key infrastructure of the project PRESERVE [9]. Section VII concludes the paper and gives an outlook for future work.

II. Related Work

The problem of privacy preserving certificate management in VANETs is widely discussed and different proposals are published. The Secure Revocable Anonymous Authenticated Communication protocol (SRAAC) [10] uses magic-ink signatures with shared secret schemes in order to provide blindly signed pseudonym certificates. Using this protocol, the vehicle identity can only be resolved if a defined number of CA servers cooperate to map a pseudonym certificate to a resolution tag and subsequently to the vehicle's identity.

In [11] the authors propose a similar protocol that also blindly signs pseudonym certificates but in contrast to SRAAC, the resolution information, called V-token, is stored inside the certificate instead of storing this information in the CA's database. Both protocols require extensive message exchange in the pseudonym acquisition phase caused by the blind signature scheme.

Another credential and certificate management scheme with the possibility of pseudonym resolution is proposed as a draft version by the U.S. Department of Transportation in [12]. This framework considers also misbehavior detection and bases on the imprint of linked identifiers in the pseudonym certificates. The linking information is managed by at least two linkage authorities that both have to cooperate in order to get long-term information or pseudonym linking information.

Similar to [12], a split of duties inside a PKI between pseudonym certificate issuer and request authentication verifier is also discussed in [13] and [14]. Due to this separation, no PKI entity alone is able to link a long-term identity to the related short-term IDs. However, the resolution of pseudonyms is not recognized in both works. Similarly, the European Telecommunications Standard Institute (ETSI) specifies a PKI with different entities responsible for request authentication verification and pseudonym certificate issuance [15]. But protocols for pseudonym resolution are not included yet.

We differ from the aforementioned work by focusing on two issues of conditional pseudonym resolution in VANETs. First, our protocol does not increase the size of pseudonym certificates, and secondly, the latency in the issuance process is not increased.

III. System Model

The ITS model consists of mobile and fixed ITS stations such as vehicles, trucks, roadside stations and PKI servers in the back-end. In order to establish trust between all these entities a Root Certificate Authority (RCA) is established as trusted third party as shown in Fig. 1.

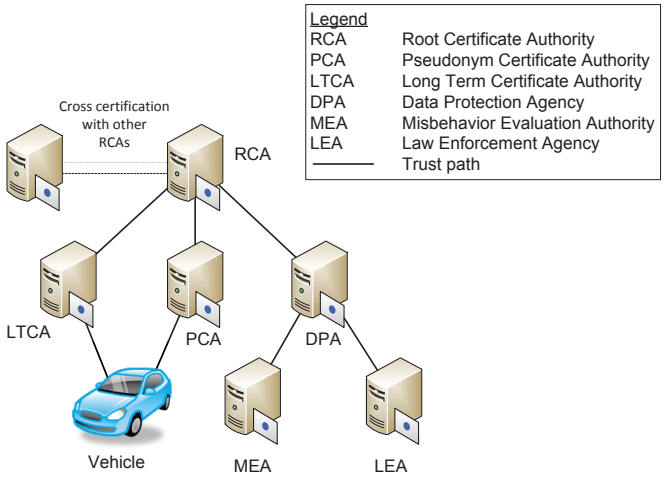

Fig. 1. Entities of the assumed PKI domain

A Long-Term CA (LTCA) is used to issue a long-term certificate for a vehicle V in the network. In order to protect the driver's privacy, the vehicles are using pseudonymous short-term certificates in the VANET communication that are issued by the Pseudonym CA (PCA). Only a vehicle that is equipped with a valid Long-Term Certificate LTC is able to obtain a short-term Pseudonym Certificate PC from an arbitrary trusted PCA as described in [14] and [15]. After certificate generation, a hashed digest of the related certificate can be calculated to get the long-term identifier id_{LTC} and short-term pseudonym identifier id_{PC} according to [3]. A pseudonym certificate includes a public key PK_{PC} that is related to the private key SK_{PC} but it contains no information linking id_{PC} to id_{LTC}. In the phase of certificate issuance, the vehicle needs to communicate with the LTCA and PCA. If a vehicle V_a communicates subsequently with another vehicle V_b, it signs outgoing messages with the private key SK_{PC_a} of a short-term pseudonym certificate PC_a and append the related signature as well as the certificate to the message. The receiving vehicle V_b is able to verify the appended certificate PC_a from V_a by checking all authorities up to the RCA in order to trust sent message data. In order to increase the efficiency, the verification of certificates can be omitted if they were previously verified. However, the message content must be verified every time using the public key PK_{PC_a} from the certificate PC_a.

A fundamental information element of the VANET communication is the position of adjacent vehicles. Therefore, a position vector can be found in every beacon message. This

vector consists of a short-term pseudonymous identifier id_{PC}, an absolute position, a heading value, the current velocity and a related timestamp of sender V which uses the certificate PC at the time interval. Based on the position vectors, every vehicle is running a local misbehavior detection system that verifies the position vector and thereby the neighbor's driving behavior [16], [6], [7] in order to identify inconsistencies and possible misbehavior. After local evaluation of suspicious behavior the vehicle creates a Misbehavior Report (MR) and sends it to a central Misbehavior Evaluation Authority (MEA) in order to identify the attacker and exclude it [8].

All involved entities of the PKI domain, as shown in Fig. 1, are equipped with certificates that are issued by a common trusted root CA. Based on a policy, the RCA puts permissions and authorization information into the certificates that are issued for authorities that would like to resolve pseudonyms for different purposes. A Law Enforcement Agency (LEA) for example may get the permission to request the long-term identifier id_{LTC} whereby a misbehavior evaluation authority gets only the permission to request information whether different pseudonyms belong to the same vehicle. According to Fig. 1, a Data Protection Agency (DPA) issues the certificates for the LEA and MEA with appropriate permissions. As long as the PCA and LTCA are not compromised and do not collude in a malicious way, a DPA act as surveillance operator in the pseudonym resolution process.

IV. Privacy Preserving Pseudonym Resolution Protocol

The following protocol for pseudonym resolution aims to be applicable in different PKI environments to provide privacy preserving acquisition of pseudonym certificates and enables conditional resolution of pseudonyms in defined situations. Our protocol, named CoPRA, is separated into two processes: During acquisition of pseudonym certificates, resolution information has to be created and distributed as shown in Fig. 2 and detailed in Section IV-A. Subsequently, authorized authorities are allowed to request pseudonym resolution information as described in Section IV-B. In the resolution process, we further distinguish between a) identity resolution of pseudonyms and b) linkability of pseudonyms.

In case a), an authority A requests the vehicle identity id_V (e.g. license plate number or vehicle identification number) that is related to a given pseudonym PC. This identity resolution should be possible only in well defined situations, if for example a law enforcement agency needs to know the identity of a vehicle after a hit-and-run accident. For this purpose, our protocol can be used with a defined number of data protection authorities $DPA_1, ..., DPA_n$ or juridical institutions $J_1, ..., J_n$ that have to be involved in the process to get id_{LTC} and id_V. For simplicity, we consider in the following protocol discussions only one instance of a DPA.

In case b), an authority A needs to only get the information whether pseudonyms $PC_{V_{a'}}$ and $PC_{V_{a''}}$ belong to the same vehicle V_a. We propose for this linkability resolution a Pseudonymous Long-Term identifier PLT that can be used by a misbehavior evaluation authority to identify vehicles that fake misbehavior events and reports. This kind of resolution may have lower privacy protection requirements, as id_V is not disclosed and PLT can change regularly. Nevertheless, data protection authorities $DPA_1, ..., DPA_n$ can also be integrated in the pseudonym linkability resolution process.

A. Pseudonym Acquisition

The basic protocols for requesting pseudonym certificates from the PKI are described in [14] and follow standardized ETSI specifications [15]. In general, a split of powers between the enrollment authority (LTCA) and the pseudonym certificate provider (PCA) is proposed due to privacy protection requirements inside the PKI. The standard protocols are extended in our proposal in order to make conditional and temporal restricted pseudonym resolution possible. An overview of the protocol is provided in Fig. 2 and detailed in Fig. 3, whereby the numbers in Fig. 2 are related to the steps in Fig. 3. The protocol shows the enrollment of vehicles as well as the acquisition of pseudonym certificates.

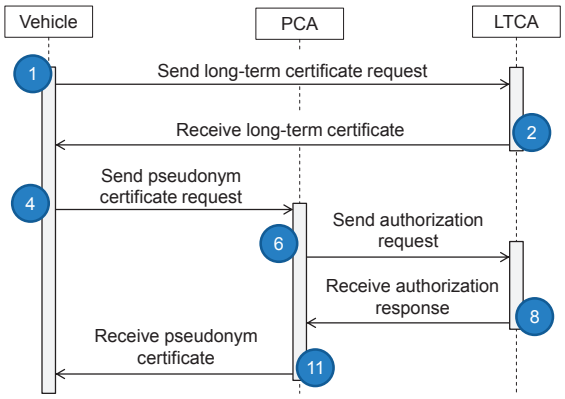

Fig. 2. Overview of certificate acquisition

We propose a protocol that bases on the well known idea of separation of duties [12], [15] in order to protect the identity of vehicles and drivers and ensure unlinkability of pseudonym certificates.

1) Enrollment phase: Every vehicle of the VANET has to be equipped with valid certificates in order to communicate with other ITS stations. Therefore, the vehicle V has to be enrolled at a LTCA in order to get a valid long-term certificate LTC_V. Details of the enrollment should be left unspecified in this protocol as vehicle manufacturers may have specific solutions to register their ITS station in a secure manner. Nevertheless, in the first step (1) the enrollment process shall consider authentication, authorization, integrity and non-repudiation of the requesting ITS station in order to prevent enrollment of malicious stations. If this can be assumed the LTCA generates and issues in (2) a new long-term certificate LTC_V based on the given public key PK_{LTC_V}. We indicate a signature with the private key SK_{LTCA} over a whole content with $\sigma_{LTCA}(\circ)$. The resulting certificate is sent to V and can be used subsequently to request pseudonym certificates.

Enrollment phase:

$$V \rightarrow LTCA \quad : \quad (id_V, PK_{LTC_V}) \tag{1}$$

$$V \leftarrow LTCA \quad : \quad LTC_V = (PK_{LTC_V}, id_{LTCA}, \sigma_{LTCA}(\circ)) \tag{2}$$

Pseudonym acquisition phase:

$$V \quad : \quad req = (PK_{PC_V}, E_{PK_{LTCA}}(id_{LTC_V})) \tag{3}$$

$$V \rightarrow PCA \quad : \quad (req, \sigma_{LTC_V}(req)) \tag{4}$$

$$PCA \quad : \quad RId_{PC_V} = (\delta(PK_{PC_V})||rand) \tag{5}$$

$$PCA \rightarrow LTCA \quad : \quad (\sigma_{LTC_V}(req), \delta(req), RId_{PC_V}, E_{PK_{LTCA}}(id_{LTC_V}), \sigma_{PCA}(\circ)) \tag{6}$$

$$LTCA \quad : \quad store(RId_{PC_V}, id_{LTC_V}, id_{PCA}) \tag{7}$$

$$PCA \leftarrow LTCA \quad : \quad (\delta(req), exp_{PC_V}, \sigma_{LTCA}(\circ)) \tag{8}$$

$$PCA \quad : \quad PC_V = (PK_{PC_V}, id_{PCA}, \sigma_{PCA}(\circ)) \tag{9}$$

$$PCA \quad : \quad store(id_{PC_V}, RId_{PC_V}, id_{LTCA}) \tag{10}$$

$$V \leftarrow PCA \quad : \quad PC_V \tag{11}$$

Fig. 3. Protocol for issuing long-term and pseudonym certificates

2) Pseudonym acquisition phase: The protocol for pseudonym certificate acquisition bases on a split of duties between enrollment authority (LTCA) and short-term pseudonym certificate provider (PCA) as proposed in [14]. Vehicle V creates in (3) a pseudonym certificate request that contains the public key of a freshly generated asymmetric key pair (PK_{PC_V}, SK_{PC_V}) and the long-term ID id_{LTC_V} that is encrypted with the public key PK_{LTCA} of the LTCA using an Integrated Encryption Scheme (IES). The private key SK_{PC_V} is stored securely in the ITS station and must never leave it. (4) This request is signed with the long-term certificate proving identity id_{LTC_V} and subsequently sent to a PCA. (5) The PCA generates a resolution identifier RId_{PC_V} related to the requested pseudonym PC_V by composing the hashed digest $\delta(PK_{PC_V})$ of the given public key PK_{PC_V} and a random $rand$. Inside the PCA domain, RId has to be unique. As the PCA is not able to verify the signature $\sigma_{LTC_V}(req)$ of the pseudonym request, due to the encrypted long-term ID id_{LTC_V}, the request is forwarded to the appropriate LTCA. (6) This authentication request consists of the request signature $\sigma_{LTC_V}(req)$ created by V, a hash digest of the request $\delta(req)$ created by the PCA, the resolution ID RId_{PC_V}, and the encrypted long-term ID $E_{PK_{LTCA}}(id_{LTC_V})$. The PCA signs the authentication request with SK_{PCA} to prove its ownership. We indicate a signature over the whole message with $\sigma(\circ)$. The LTCA decrypts id_{LTC_V} using SK_{LTCA} and verifies $\sigma_{LTC_V}(req)$ with the appropriate public key PK_{LTC_V} to check the correctness of the pseudonym certificate request. Furthermore, the desired pseudonym certificate information like expiration time and permissions are checked by the LTCA. (7) In case of positive verification, the resolution ID RId_{PC_V} is stored in a database of the LTCA linked to the respective long-term ID id_{LTC_V} and PCA identifier id_{PCA}. The verification result is further used to generate an appropriate response for the PCA. (8) This response contains, in case of successful verification, a hashed digest of the original pseudonym request $\delta(req)$ and expiration information exp_{PC_V} of the new pseudonym certificate. The whole response message is signed by the LTCA using SK_{LTCA} to prove its possession. (9) After verification of the returned authentication request, the PCA creates a new pseudonym certificate PC and stores the previously generated resolution ID RId_{PC_V} in a database together with the related id_{PC_V} and id_{LTCA} in (10). Finally, the pseudonym certificate PC_V is transmitted to the vehicle in (11).

In order to protect the communication against manipulation and eavesdropping, all data transmitted between the entities in the proposed protocol is encrypted with an IES (e.g. ECIES [17]). Hereby, the sender of a message generates an asymmetric key pair $(PK_{s,r}, SK_{s,r})$ and a symmetric key $K_{s,r}$. This set of keys is only used to protect the message transport between a specific sender s and a receiver r in a session. According to [17], the transmitted message is first encrypted with the symmetric key $K_{s,r}$ and subsequently $K_{s,r}$ is encrypted with the public key of the receiver PK_r. This strategy makes atomic communication between the entities (i.e. vehicle, PCA, and LTCA in Fig. 3) possible without establishing complex sessions with multiple exchange of packets.

B. Conditional Pseudonym Resolution

Vehicles that are equipped with valid pseudonym certificates are able to use them in VANET communication. In case of misbehavior detection or critical traffic situations (i.e. car accidents) the resolution of the pseudonymous short-term identifier may be necessary. The protocol shown in Fig. 4 and detailed in Fig. 5 allows linking of different pseudonyms or providing the respective long-term ID of a pseudonym. Based on policies, the LTCA is able to provide different

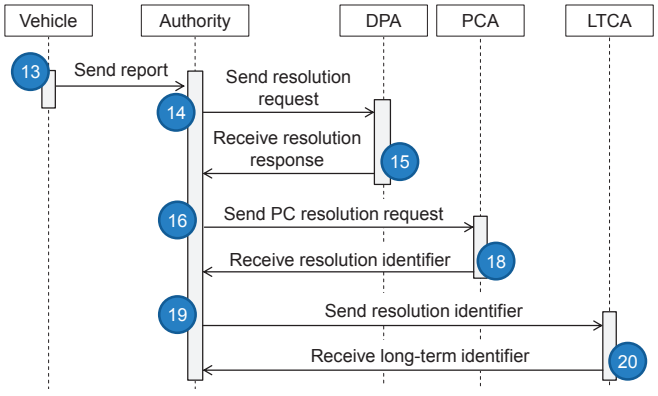

Fig. 4. Overview of pseudonym certificate resolution

resolution information to an interested authority A. A misbehavior evaluation authority MEA may need only temporary

linking information of pseudonyms $PC_1, ..., PC_n$ in form of a pseudonymous long-term ID id_{PLT}. Whereupon, a law enforcement agency may need to know the non-pseudonymous long-term ID id_{LTC_V} of PC_V in order to request additional information id_V regarding V. For our protocol description in Fig. 5, we assume the request of the long-term ID id_{LTC_V} by authority A in which a DPA must be involved as attesting notary. During communication in the VANET, vehicle V_a or other ITS stations are able to record short-term IDs id_{PC_V} from received messages. (12) According to the motivation of V_a, a message msg is created that contains the short-term ID $id_{PC_{V_b}}$ of a vehicle V_b which is involved in an event that triggers generation of msg. Additionally, a signed record of vehicle V_b is appended to msg that motivates the pseudonym resolution. This could be for example a broadcasted message containing a position vector proving the existence of V_b at the specific time and position. For simplicity, we add in (12) only

$$
\begin{aligned}
V_a &: msg = (list(id_{PC_{V_b}}, record_{V_b}, \\
&\quad \sigma_{PC_{V_b}}(record_{V_b})), \sigma_{PC_{V_a}}(\circ)) && (12)\\
V_a \rightarrow A &: msg && (13)\\
A \rightarrow DPA &: (msg, id_{PC_{V_b}}, rt, \sigma_A(\circ)) && (14)\\
A \leftarrow DPA &: res_{DPA} = (\delta(msg, id_{PC_{V_b}}), t_c, \\
&: rt, \sigma_{DPA}(\circ)) && (15)\\
A \rightarrow PCA &: (msg, id_{PC_{V_b}}, res_{DPA}, rt, \sigma_A(\circ)) && (16)\\
PCA &: eRId = E_{PK_{LTCA}}(RId_{PC_{V_b}}, \\
&: \delta(msg, id_{PC_{V_b}}), t_e) && (17)\\
A \leftarrow PCA &: res_{PCA} = (\delta(msg, id_{PC_{V_b}}), eRId, \\
&\quad rt, res_{DPA}, \sigma_{PCA}(\circ)) && (18)\\
A \rightarrow LTCA &: (res_{PCA}, \sigma_A(\circ)) && (19)\\
A \leftarrow LTCA &: (\delta(msg, id_{PC_{V_b}}), id_{LTC_{V_b}}, \\
&: t_{exp}, \sigma_{LTCA}(\circ)) && (20)
\end{aligned}
$$

Fig. 5. Protocol for conditional pseudonym resolution

one pseudonym that should be resolved. Depending on the purpose, additional short-term IDs with related records can be added to the message msg. Before the message is provided to an authorized authority A in (13), the whole message content is signed with the private key of a PC of V_a indicated by $\sigma_{PC_{V_a}}(\circ)$ in our protocol. (14) Based on regulations, defined in a policy, the pseudonym resolution request must optionally be supported by other entities (e.g. data protection agencies DPA). If this support is needed, authority A extracts the pseudonym PC_{V_b} that should be resolved and forwards the original message along with $id_{PC_{V_b}}$ to the respective DPA. Furthermore, the desired resolution type rt (e.g. full identity resolution or pseudonym linking information) is appended. The whole request is signed with the private key SK_A of the authority. Subsequently, the DPA verifies the signature with the public key PK_A and checks whether A is authorized to request pseudonym resolution information from the PKI. (15) If the DPA supports the resolution request, a digest δ of request data is generated by using a hash function. Subsequently, the digest, the current time t_c, and the confirmed resolution type rt are signed and sent to A. (16) After receiving the response from the supporting authority, A sends msg, $id_{PC_{V_b}}$ and the confirmation from DPA, signed with its private key SK_A, to the PCA. (17) The PCA verifies and checks the signatures and permissions of A and DPA and gets the appropriate resolution ID $RId_{PC_{V_b}}$ from its database. In order to prevent misuse of $RId_{PC_{V_b}}$, it is encrypted with the public key of the related LTCA. (18) Subsequently, the PCA generates a response with the digest of message msg and the pseudonym ID $id_{PC_{V_b}}$ that should be resolved, the encrypted resolution ID $RId_{PC_{V_b}}$ and the confirmation of DPA. The whole response is signed and sent to A. (19) When A receives the data from the PCA, the response res_{PCA} is signed by A and sent to the appropriate LTCA. The ID of the responsible LTCA can be extracted from the encryption header of $eRId$. (20) First, the LTCA verifies all signatures and certificates from A, DPA and PCA as well as permissions contained in the respective certificates. Afterwards, the LTCA checks that all contained digests $\delta(msg, id_{PC_{V_b}})$ are equal. The kind of pseudonym resolution is based on the type that must be confirmed by the DPA and the PCA. In the presented protocol we assume a request for full identity resolution. Therefore, the LTCA provides the long-term identifier $id_{LTC_{V_b}}$ that is linked to the given resolution ID $RId_{PC_{V_b}}$. The timestamp t_{exp} denotes the expiry date of the provided long-term identifier. In order to guarantee authenticity and integrity of this information a signature is created by the LTCA over the whole responded data, indicated by $\sigma_{LTCA}(\circ)$.

V. Attacker Model and Security Analysis

In our attacker model, we assume that a single attacker or multiple cooperating attackers that have only access to pseudonymous information (e.g. PC_V, id_{PC_V} or RId_{PC_V}) aim to get uncontrolled access to the long-term information of a specific vehicle. Alternatively, an attacker aims to get only pseudonym linking information in order to track a specific vehicle within the VANET.

As result, we propose CoPRA that provides a flexible mechanism to conditionally resolve pseudonyms without affecting the privacy of other pseudonyms. Due to the split of duties, one entity alone cannot threaten privacy by linking arbitrarily pseudonyms to the long-term certificate. As PCA and LTCA can verify independently the correctness of requests according to local policies, malicious authorities cannot get arbitrarily resolution information. Only if the following authorities cooperate an unauthorized request would be possible:

- PCA and LTCA are compromised and maliciously cooperate. If both CA types are compromised, a database can be created where both CAs collect linking information between issued pseudonym certificates and related long-term certificates. In this case, the PCA and LTCA are not following the acquisition protocol shown in Fig. 3.

- Authority A, DPA, and PCA are compromised and maliciously cooperate. Assuming the PCA is compromised, arbitrary resolution IDs can be extracted from its database. We propose therefore independent monitoring instances A and $DPA_1, ..., DPA_n$.
- V_a, A, and DPA are compromised and maliciously cooperate. The report of faked events by V_a is considered in that way, that resolution information is provided based on the event type. Messages msg containing a misbehavior report should only be usable to get pseudonymous long-term IDs and messages msg stating a traffic fatality (e.g. hit-and-run offense) need support by external authorities $DPA_1, ..., DPA_n$ and manual interaction.

The introduction of vulnerabilities to central PKI entities is another aspect that should be analyzed. We discuss resistance of our protocol against important threats: Replay attack, Denial of Service (DoS). The replay of resolution requests sent by external attackers can be detected and directly filtered out at all entities. A digest $\delta(msg, id_{PC_{V_b}})$ is used in this case as unique identifier of a resolution task. It has to be further considered that the $record_{V_b}$, which is part of a message msg, contains variable position data and timestamps. Finally, all messages transmitted between the vehicle, authority A, DPA, PCA and LTCA are signed and encrypted.

The DoS attacks on involved entities can be limited due to the usage of digital signatures. Requests and responses are only accepted and processed if the signature is valid. Therefore, an attacker must spend cryptographic effort in signing operations to mount a DoS attack. Indeed, an attacker could flood the authorities with invalid signed messages. A possible countermeasure is the checking of the sender's certificate first and handle unknown and untrusted senders with lower priority.

VI. Application for Misbehavior Detection

For a misbehavior detection and evaluation system it is necessary to get pseudonym linking information in order to identify attackers in ITS communication. A central Misbehavior Evaluation Authority (MEA) collects Misbehavior Reports (MR) from ITS stations of the VANET. As vehicles can change their pseudonyms arbitrarily, it is a major requirement of a MEA to check whether PCs belong to the same ITS station.

The structure of a misbehavior report, shown in Fig. 6, contains the type of detected misbehavior, the pseudonymous ID $id_{PC_{V_a}}$ of the reporter node, a list of suspected nodes including their pseudonym IDs $id_{PC_{V_b}}$ and a list of relevant neighbor nodes surrounding the reporter. In every report an

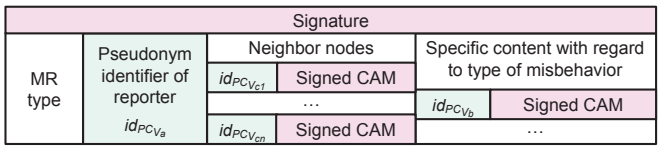

Fig. 6. Structure of misbehavior report

evidence of the misbehavior should be added in form of signed CAMs that attest the existence of the node at the claimed position and time. This signed CAM is used in the protocol by the PCA and possible involved DPAs to verify that a resolution request is justified.

The MEA is further equipped with a certificate that contains permissions to request pseudonym linking information. The certificate of the MEA is issued by a root CA that is trusted by all other involved entities as depicted in Fig. 1. Based on the permission contained in the MEA certificate and policies at the PCA and LTCA, a pseudonymous and timely limited identifier PLT is provided by the LTCA. This can be used by the MEA to check if pseudonyms belong to the same sender.

A. Pseudonym Linking for Central Misbehavior Evaluation

The protocol presented in Fig. 7 uses specific data for misbehavior evaluation but follows the generic protocol described in Fig. 5. In order to balance the system cost, the integration of a DPA is not mandatory for temporal pseudonym linking resolution. However, its integration could be done easily if needed as described in the generic protocol in Section. IV-B. A vehicle V_a generates in step (21) a MR that contains pseudonymous identifiers of involved ITS stations as depicted in Fig. 6 and sends it to the MEA. The received MR is used by the MEA to generate a resolution request in step (22) that is sent to the PCA. We assume in this example that no support of DPAs is required. Based on the MR content, the PCA decides whether the desired resolution type rt is accepted and encrypts the resolution ID (23). The response, that is sent to the MEA in step (24) contains a digest $\delta(MR, id_{PC_{V_b}})$, the encrypted resolution ID and the resolution type. This data is signed by the MEA in (25) and sent to the LTCA. Based on rt,

$$
\begin{aligned}
V_a &: MR = (list(id_{PC_{V_b}}, CAM_{V_b}, \\
&\quad \sigma_{PC_{V_b}}(CAM_{V_b})), \sigma_{PC_{V_a}}(\circ)) && (21)\\
MEA \rightarrow PCA &: (MR, id_{PC_{V_b}}, rt, \sigma_{MEA}(\circ)) && (22)\\
PCA &: eRId = E_{PK_{LTCA}}(RId_{PC_{V_b}}, \\
&: \delta(MR, id_{PC_{V_b}}), t_e) && (23)\\
MEA \leftarrow PCA &: res_{PCA} = (\delta(MR, id_{PC_{V_b}}), \\
&\quad eRId, rt, \sigma_{PCA}(\circ)) && (24)\\
MEA \rightarrow LTCA &: (res_{PCA}, \sigma_{MEA}(\circ)) && (25)\\
LTCA &: PLT_{PC_{V_b}} = (id_{LTC_{V_b}} || r || t_{exp}) && (26)\\
MEA \leftarrow LTCA &: (\delta(MR, id_{PC_{V_b}}), PLT_{PC_{V_b}}, t_{exp}, \\
&: \sigma_{LTCA}(\circ)) && (27)
\end{aligned}
$$

Fig. 7. Protocol for temporal restricted pseudonym resolution

the LTCA creates a temporal restricted pseudonymous long-term ID in step (26). This identifier $PLT_{PC_{V_b}}$ is a composed one way hash value containing the long-term ID $id_{LTC_{V_b}}$, a random value r and the expiration time t_{exp}. In (27) finally, the digest δ, the resolution ID, and the expiration time of PLT is responded. In order to guarantee authenticity and integrity of this information a signature is created by the LTCA over the whole responded data.

B. Comparison of Pseudonym Resolution Protocols

Table I compares the CoPRA protocol with related schemes for pseudonym resolution in the context of misbehavior detection in ITS communications. In the first row, the effect of pseudonym resolution is compared by means of overhead in pseudonym certificates. As pseudonyms are appended to messages in the wireless communication, the overhead should be as small as possible.

TABLE I
COMPARISON OF PSEUDONYM RESOLUTION SCHEMES FOR VANETS

Topic of comparison	V-Token [11]	SRAAC [10]	CoPRA
Overhead in pseudonym certificate	$\geq$ 61 Bytes	0 Bytes	0 Bytes
Certificate acquisition overhead at CA	0 Bytes	$\geq$ 64 Bytes per cert.	$\geq$ 8 Bytes per cert.
Certificate acquisition performance	DSS encryption operation	shared secret interpolations (e.g. [18])	no additional overhead
Certificate acquisition connection type (vehicle $\leftrightarrow$ PCA)	session based (blind signature) [19], [20]	session based (MI-DSS*) [21]	atomic
Certificate resolution overhead	$\geq$ 61 Bytes	$\geq$ 64 Bytes	$\geq$ 1 KB
Certificate resolution performance	shared secret interpolations (e.g. [18])	shared secret interpolations (e.g. [18])	DSS sign and verify operations

The second row shows the amount of data that needs to be stored at the CAs in order to support pseudonym resolution. In contrast to the V-Token protocol, SRAAC and CoPRA manage the resolution information centrally by storing data in a database. In the third row, the certificate acquisition performance is compared. Here, we consider only operations that are necessary to add resolution information in form of a *V-Token* in [11], a *Tag* in [10] and *Resolution-Id* in CoPRA. In contrast to the related protocols, our scheme entails no cryptographic operations for resolution information generation and storage. The type of connection between vehicle and pseudonym provider is compared in the fourth row. As discussed in Section I, the request of pseudonym certificates from the PKI should be packet based. This allows interruption of pseudonym acquisition with later continuation. In row 5 and 6, the overhead and performance in the resolution process is compared. As shown in Table I, our conditional pseudonym resolution protocol does not decrease wireless vehicular communication performance as no additional data is added to pseudonym certificates. Also no additional cryptographic operations are introduced in the pseudonym acquisition phase. We used for evaluations a testbed PKI implementation based on IEEE 1609.2 [3] with LTCA - PCA server separation, running on a quad core CPU with 2.7 GHz. Using this environment, the processing of one pseudonym certificate request takes 179 ms at the CAs and the processing of a request with 50 public keys requires approximately one second. Avoiding additional delay in the pseudonym acquisition phase is important as every vehicle in the network requests regularly hundreds of certificates. The storage of resolution information is in the magnitude of Megabytes and therefore not critical also when several million pseudonym are issued by the PKI. According to row 5 and 6 of Table I, our protocol entails several bytes of data that have to be transmitted between involved entities. Additionally, several signing and verification processes are necessary. But the conditional resolution of pseudonyms is performed relatively seldom compared to the pseudonym acquisition process.

C. Performance Analysis of Pseudonym Resolution

Using the use-case of misbehavior detection, the MEA must check whether identifiers in a misbehavior report belong to separate vehicles. Otherwise, an attacker would be able to send faked misbehavior reports in order to blacklist arbitrary ITS stations. Fig. 8 shows the latency in milliseconds of pseudonym resolution processes on the y-axis. On the x-axis the number of pseudonyms to be resolved, contained in a single request, is shown. As discussed in section VI, a misbehavior report usually contains several pseudonyms id_{PC} from different vehicles (i.e. reporter, suspected nodes, witnesses). In order to prevent misuse and blackmailing, the linkability of involved pseudonyms has to be checked. In Fig.

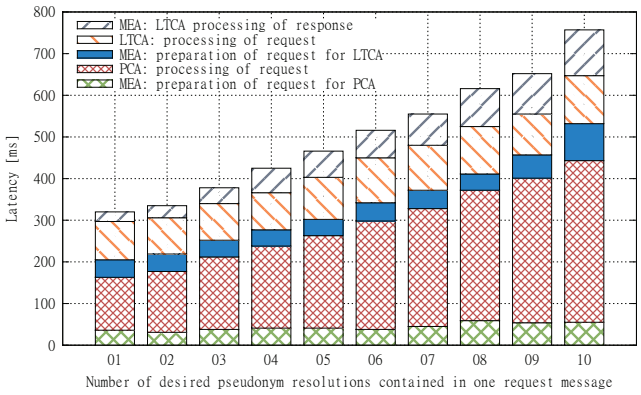

Fig. 8. Latency distribution in pseudonym resolution with empty database

8, the measured latency at involved PKI entities is shown. According to the protocol described in Section VI-A, the MEA prepares the pseudonym resolution request and sends it to the PCA. Then the PCA checks the content of the request by verifying the contained misbehavior report with included CAMs. This step mainly causes the increase of latency at the PCA with increasing number of desired PC resolutions. The remaining operations at the MEA and LTCA are relatively static. General overhead for every pseudonym resolution is introduced by DSS operations in the protocol. Every message between MEA, PCA and LTCA is signed and encrypted at the sender and decrypted and verified at the receiver using ECDSA and ECIES according to [3].

Fig. 9 shows the latency in the pseudonym resolution process with different number of database entries at the MEA, PCA and LTCA. We measured the mean, maximum and minimum latency, as shown on the y-axis, in relation to an increasing number of desired PC resolutions on the x-axis. The more pseudonym certificates are issued by the PCA and LTCA

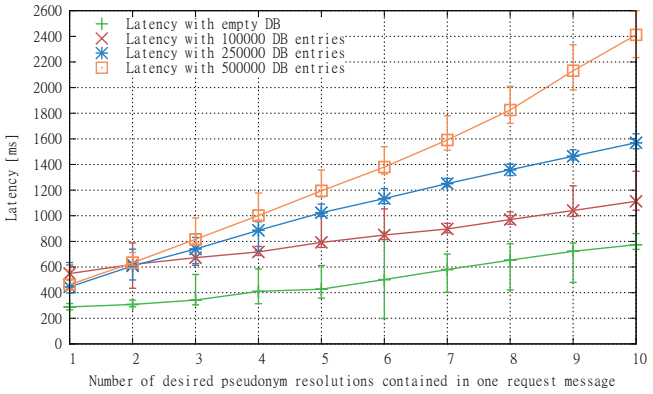

Fig. 9. Latency of pseudonym resolution related to database size

the more database entries are necessary to store the relation between pseudonym ID and resolution ID in the database. As result, the delay for searching the database is increased. But according to Fig. 8 and Fig. 9, a PKI is able to process approximately 250 pseudonym resolution requests per minute, even if the database is filled. This is sufficient for automated central misbehavior evaluation [8].

VII. Conclusion and Outlook

We propose in this paper a protocol for conditional pseudonym resolution in VANETs that prevents misuse and preserves privacy and unlinkability of remaining pseudonyms. Focusing on the use-case of misbehavior detection, we have shown that conditional pseudonym resolution is possible without increase of certificate size and therefore increase of bandwidth requirements for wireless communication channels. Our proposed protocol is a balanced solution between full anonymity and uncontrolled arbitrary access to privacy related information (i.e. pseudonym certificate information). The design of our protocol is flexible in order to handle different types of resolution requests motivated by different intentions, for example lawful interception, misbehavior detection and attacker identification or evaluation of field operational tests. The security analysis has shown the strength of CoPRA as unintended access to pseudonym resolution information is only possible if several CAs, ITS stations and infrastructure agencies cooperate in a malicious way. Our implementation and performance measurements have further shown that CoPRA is not increasing the delay and overhead of pseudonym acquisition and has adequate performance for providing pseudonym resolution information for misbehavior detection and evaluation.

In future work, CoPRA could be extended by trusted computing mechanisms in order to enforce the conformance to the proposed protocols. A policy enforcement scheme could be applied as middleware between CA software and database to restrict and control access to sensitive data.

Acknowledgment

The research leading to these results has received funding from the European Union's Seventh Framework Programme project PRESERVE under grant agreement n°269994.

References

[1] ETSI - European Telecommunications Standards Institute, "Intelligent transport systems (ITS); vehicular communications; basic set of applications; part 2: Specification of cooperative awareness basic service," ETSI, Technical Standard TS 102 637-2, April 2010.

[2] SAE International TM, "Surface vehicle standard - dedicated short range communications (DSRC) message set dictionary," SAE J2735, Tech. Rep., November 2009.

[3] IEEE Computer Society, "Draft standard for wireless access in vehicular environments - security services for applications and management messages," Institute of Electrical and Electronics Engineers, Draft Standard IEEE P1609.2/D12, January 2012.

[4] ETSI - European Telecommunications Standards Institute, "Intelligent transport systems (ITS); security; stage 3 mapping for ieee 1609.2," ETSI, Technical Standard TS 102 867, 2011.

[5] A. Pfitzmann and M. Hansen, "A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management," August 2010, v0.34.

[6] N. Bißmeyer, C. Stresing, and K. Bayarou, "Intrusion detection in VANETs through verification of vehicle movement data," in *Second IEEE Vehicular Networking Conference*. IEEE, December 2010.

[7] R. K. Schmidt, T. Leinmueller, E. Schoch, A. Held, and G. Schaefer, "Vehicle behavior analysis to enhance security in VANETs," in *Proceedings of the 4th IEEE Vehicle-to-Vehicle Communications Workshop (V2VCOM2008)*, 2008.

[8] N. Bißmeyer, J. Njeukam, J. Petit, and K. Bayarou, "Central misbehavior evaluation for vanets based on mobility data plausibility," in *VANET '12: International workshop on Vehicular inter-networking*. ACM, April 2012.

[9] N. Bißmeyer, J. Petit, D. Estor, M. Sall, J. P. Stotz, M. Feiri, R. Moalla, and S. Dietzel, "PRESERVE d1.2 v2x security architecture," PREparing SEcuRe VEhicle-to-X Communication Systems Consortium, Deliverable, November 2011.

[10] L. Fischer, A. Aijaz, C. Eckert, and D. Vogt, "Secure revocable anonymous authenticated inter-vehicle communication (SRAAC)," in *4th Conference: escar - Embedded Security in Cars*, Germany, 2006.

[11] F. Schaub, F. Kargl, Z. Ma, and M. Weber, "V-tokens for conditional pseudonymity in VANETs," in *IEEE Wireless Communications and Networking Conference (WCNS)*, 2010.

[12] U. D. of Transportation Research and I. T. Administration, "Security credential management system design security system design for cooperative vehicle-to-vehicle crash avoidance applications using 5.9 ghz dedicated short range communications (dsrc) wireless communications," CAMP, VSC3, www.its.dot.gov, Tech. Rep., February 2012.

[13] S. Pietrowicz, T. Zhang, and H. Shim, "Short-lived, unlinked certificates for privacy-preserving secure vehicular communications," in *17th ITS World Congress*. ITS America, October 2010.

[14] N. Bißmeyer, J. P. Stotz, H. Stübing, E. Schoch, S. Götz, and B. Lonc, "A generic public key infrastructure for securing car-to-x communication," in *18th World Congress on Intelligent Transportation Systems*. ITS America, October 2011.

[15] ETSI - European Telecommunications Standards Institute, "Intelligent transport systems (ITS); security; security services and architecture," ETSI, Technical Standard TS 102 731, September 2010.

[16] A. Jaeger, N. Bißmeyer, H. Stübing, and S. A. Huss, "A novel framework for efficient mobility data verification in vehicular ad-hoc networks," *International Journal of ITS Research, ITS Japan*, vol. 9, no. 3, September 2011.

[17] IEEE Computer Society, "IEEE standard specifications for public-key cryptography- amendment 1: Additional techniques," *IEEE Std 1363a-2004 (Amendment to IEEE Std 1363-2000)*, pp. 1 –159, 2004.

[18] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, no. 11, pp. 612–613, November 1979. [Online]. Available: http://doi.acm.org/10.1145/359168.359176

[19] D. Chaum, "Blind siganture systems," US Patent 4 759 063, July, 1988.

[20] D. Jena, S. K. Jena, and B. Majhi, "A novel untraceable blind signature based on elliptic curve discrete logarithm problem," *IJCSNS*, vol. 7, no. 6, pp. 269–275, June 2007.

[21] M. Jakobsson, "Privacy vs. authenticity," PhD Thesis, University of California, San Diego, 1997.