Bionyms: Driver-centric Message Authentication using Biometric Measurements

Marc Roeschlin, Christian Vaas, Kasper B. Rasmussen, and Ivan Martinovic
University of Oxford, Oxford, United Kingdom
{firstname.lastname}@cs.ox.ac.uk

***Abstract*—The technology of self-driving cars and driver-assistance systems has reached a point where vehicles start to make decisions on behalf of drivers and operate autonomously. The introduction of Vehicular Ad-hoc Networks (VANETs) will increase this autonomy to greatly improve efficiency and safety on the road. However, when relying on vehicle-to-vehicle communication to make life-critical decisions, such as emergency braking, information authenticity and integrity is of paramount importance. Current schemes that satisfy these properties tie the identity of a vehicle's owner to its messages and discourage malicious behavior under the penalty of prosecution. But if driver and owner are not the same, it is difficult to identify the person causing an accident or committing a traffic offense. This is particularly relevant for increasingly popular car sharing schemes and Transportation as a Service (TaaS) where vehicles are owned by mobility providers. In this paper, we propose a novel message authentication scheme based on biometric information that provides traceability of each message to the driver. This enables accountability and exclusion from the network on a per-individual basis, while at the same time preserving driver privacy. To evaluate functional protocol properties, such as computation overhead, we simulate traffic in a realistic road network. We implement our scheme and demonstrate its feasibility using a driver's body impedance, an unobtrusive biometric modality that can be acquired while holding the steering wheel. Our evaluation is supported by data gathered in a user study with 33 subjects conducted under simulated driving conditions.**

I. Introduction

Vehicular Ad-hoc Networks (VANETs) are a cornerstone for the next generation of transportation. The IEEE 802.11p [1] transmission standard allows the wireless exchange of information among vehicles' On-Board Units (OBUs) and stationary Road-Side Units (RSUs). This facilitates safety applications, such as cooperative collision avoidance, as well as increases efficiency through, e.g., cooperative adaptive cruise control. However, due to the broadcast nature, messages can be received by anyone within a 300 meter perimeter. While this provides situational awareness, it introduces security and privacy challenges; VANETs have to provide message authenticity and integrity to prevent the injection of false information which jeopardizes the safety of passengers. For example, spoofing vehicle coordinates can create fictive congestion and trigger the collision avoidance system of individual vehicles. On the contrary, messages containing location information, such as mandatory Cooperative Awareness Messages (CAMs) allow to track vehicles [2]. Consecutive messages from the same vehicle can leak information such as its itinerary or even the identity of the driver [3]. Hence, it is necessary for messages not to carry identifying information so that drivers remain anonymous.

In order to secure V2V/V2I (V2X) communication, existing proposals suggest the use of vehicle-specific signing material. For privacy protection, these approaches rely on either disguising a vehicle's identity through proxy identifiers or using cryptography to provide sender anonymity. Schemes of the first type have been categorized as pseudonym-based [4], where a trusted authority assigns a set of private/public key pairs to every registered vehicle. The second type, on the other hand, utilizes identity-based or symmetric cryptography, enabling vehicles to generate anonymous signatures [5].

Independent of the underlying scheme, there is a major deficiency: the cryptographic material used to sign messages is tied to a vehicle and the owner is held accountable for the transmitted messages. This is particularly problematic for company cars, rental cars, and Transportation as a Service (TaaS). However, exactly these applications are projected to show an annual growth of over 30%, as cities in Europe aim to make it unnecessary to own a private car in the next decade [6]. At the moment, car sharing schemes are in charge of keeping track of the identity of a driver, which requires users to provide identifying personal details for every journey while they could otherwise remain anonymous if they owned a car themselves.

Undoubtedly, a VANET infrastructure that can provide fine-grained message verification while providing accountability would allow to relax privacy intruding procedures as they are currently needed. We suggest the integration of biometric measurements into the message authentication mechanism. Even though research and industry have identified the use of biometrics in the automotive context, such as for access control and immobilizers, existing proposals for biometric-enabled message authentication do not meet today's requirements for VANETs (see Sec. II). Trying to remedy those deficiencies, we follow a completely new approach based on a commitment scheme to use anonymized biometric measurements.

- Using repeatedly measured biometric traits during vehicle operation, we propose a message authentication scheme that implements the issuance and revocation of key material on a per-individual basis.
- We instantiate our solution using body impedance as the biometric modality and conduct a user study with 33 subjects using a prototype set-up.
- We provide a thorough analysis, to evaluate the security and privacy properties of the proposed protocols.
- We run simulations on a real-world road network to assess the performance of our scheme.

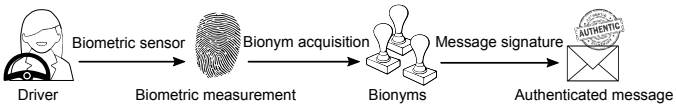

Fig. 1. Information flow: A driver requests bionyms by providing her biometric measurements. The bionyms are anonymized signing material that is used to generate VANET message signatures.

II. Related Work

Previous work that mentions the use of biometrics in conjunction with VANETs can be found in [7], [8], [9]. These pioneer the idea of enhancing driver authentication by incorporating biometric measurements in message signatures.

The authors of [7] propose to enhance user authentication in VANETs using face and fingerprint biometrics. They layer the two biometric modalities to derive a key and encrypt messages using the Exclusive-Or operation. The computational overhead and authentication time of their approach is evaluated in a scenario with roadside units, authentication servers, and up to 100 simulated vehicles. However, since the protocol uses an XOR cipher it allows an adversary to recover the biometric material via a chosen plaintext attack. This violates privacy by facilitating tracking but also enables the attacker to sign messages on behalf of the victim. Furthermore, the absence of revocation and traceability combined with a fixed message size renders the protocol unusable.

The scheme in [8] offers mutual authentication using vehicle movement. The authors suggest a Keberos-like method by replacing symmetric with biometric encryption. Without giving a description of how the biometric information is embedded into the protocol, this scheme is not ready for use.

The biometrics-based anonymous authentication presented in [9] uses biometric encryption and suggests temporary MAC addresses for privacy protection. Every pair of vehicles establishes a separate communication session that makes message broadcasting redundant, but at the same time introduces overhead quadratic to the number of communicating vehicles. In addition to that, establishment and exchange of symmetric keys are not specified and the use of biometrics is not motivated. In a simulation, the authors evaluate passenger privacy independent of the proposed biometric encryption scheme. Its applicability under real-world conditions remains unknown.

III. Bionym Scheme

Our proposed message signature scheme uses anonymous commitments, called *bionyms*, which are unique identifiers designed to authenticate VANET messages. Bionyms are derived from a driver's biometric characteristics following the steps shown in Fig. 1. The resulting signatures authenticate messages and tie them to the identity of the driver.

In order to acquire bionyms, the driver has her biometric characteristic measured by a sensor built into the vehicle. A request containing an anonymized biometric measurement is sent to a trusted authority to verify the driver's identity. If successful, bionyms are issued to the driver. They carry the anonymized biometric, are unlinkable, and have an expiration date. To ensure the availability of valid bionyms, a vehicle periodically refills its local repository using the VANET infrastructure. Since the duration between bionym acquisitions depends on the number of bionyms provided and their expiration date, the re-validation frequency of a driver's identity can be controlled by these parameters.

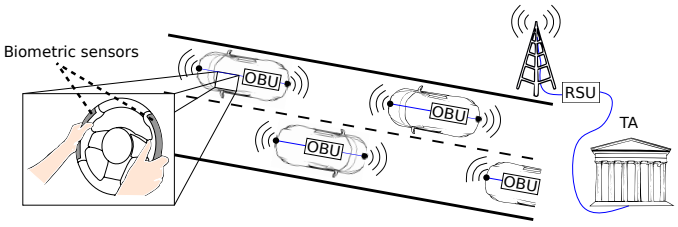

Fig. 2. System model with the three VANET entities: TA, OBUs, and RSUs. RSUs relay information between OBUs and the TA. Vehicles can acquire a driver's characteristics via sensors embedded into the steering wheel.

A. Strong Driver Authentication

Many car manufacturers offer passive key-less entry and start systems. These systems grant access to a driver's vehicle after an authentication protocol between vehicle and token was successful. However, a hardware token might be given to or stolen by another person to subvert identity verification, similarly to how a car key can be shared.

Thus, in an attempt to personalize access control, car makers have started to adopt biometrics for immobilizers and payment systems. Using a biometric trait offers the non-transferability that cannot be provided by a hardware token alone. Seamlessly acquired biometric readings allow uninterrupted driver verification throughout a journey. Otherwise, if only verified once per trip, additional measures are needed to guarantee the continuity of the driver's identity. For example, a driver's permissions would have to be invalidated immediately if an open door or window is detected. We believe that such additional indicators – especially when relying on simple sensors – are easier to circumvent than continuous biometric recognition.

We propose a combination of a possession-based and biometrics-based mechanism to prevent impersonation while providing privacy to the driver. Our scheme requires the possession of a simple token (e.g., a smart watch, bracelet or smart phone) and a biometric modality. The trust assumptions on the token are minimal, it functions as a storage for a secret used to anonymize biometric information. If not combined with biometric information, the secret is meaningless.

We do not consider a solution where the authentication process is executed on an intermediary device: If the device is wireless, special provisions are required to mitigate relay attacks, and if the device is, e.g., a smart-card, the vehicle needs an interface in addition to the biometric sensors. Furthermore, the device would have to be fully trusted and tamper-proof such that it can store biometric information in a secure way.

B. System Model

Our network model includes a Trusted Authority TA, Road-Side Units RSUs, and On-Board Units OBUs as seen in Fig. 2.

Trusted Authority: A driver enrolls at the TA and verifying her identity, the TA stores the information necessary to provide a vehicle with driver-specific *bionyms*. This process is supervised and can be combined with the issuance of a driving license.

Bionym: A bionym is a unique identifier which allows for authentication of messages sent by a vehicle. To compute message signatures, the bionym has to be combined with the driver's biometric information. We define a bionym's life-cycle in three stages: (1) acquired, (2) in use, and (3) expired. In case no bionyms are available, a vehicle has to acquire them from the TA. Thereafter, these can be used until they reach their expiration time and are no longer accepted by other vehicles.

Driver: A driver is required to enroll at the TA by providing her biometric characteristic and a second factor, e.g., a hardware token. Once the biometric measurement is stored, the ability to acquire bionyms is granted. This can be exercised using any OBU as long as the driver provides biometric measurements.

Vehicle: A vehicle's OBU includes a Hardware Security Module (HSM) that enforces the bionym life-cycle, securely stores private keys and erases excess bionyms at the end of a vehicle's journey, i.e. when the engine is turned off. An OBU is connected to the vehicle's internal bus and can access peripherals like biometric sensors. Before broadcasting a message, an OBU generates a signature using a bionym and the driver's biometric measurement.

C. Adversary Model

We consider an adversarial setting that is commonly used when analyzing VANETs: An eavesdropper who aims to reveal the location and identity of drivers by tracking them and an attacker who manipulates traffic by inserting forged messages.

In addition to the standard model, we introduce an impersonator who tries to circumvent biometric recognition.

Tracking: A passive adversary who observes VANET messages. He neither accesses, e.g., using malware, nor follows his target, e.g., by maintaining an extensive camera network, which would make tracking trivial. The adversary can, for instance, try to exploit the location information in CAMs. If the location of the victim can be derived for multiple points in time, i.e., an entire journey, chances to identify an individual are very high [10]. Generally, a tracking adversary is considered successful if he can derive an identifier directly from the messages or if the observed trip segment identifies the victim.

Traffic Manipulation: Fabricated messages can be used to adversely affect traffic, such as by reporting non-existing accidents or ghost vehicles. This creates a fictive congestion which forces drivers to slow down or even take a detour. An attacker can use this to facilitate car-jacking, robberies, or otherwise cause economic damage.

Impersonation: The adversary attempts to impersonate a driver to send VANET messages on her behalf. If the adversary is physically present in a vehicle, he can present his own or a forged biometric material to the OBU of the vehicle. If the adversary is remote, i.e., does not have access to an OBU, he can try to forge signatures by reusing captured bionyms. Either way, we assume that the adversary has not obtained a valid biometric reading of the victim and can not break the HSM part of the OBU.

Algorithm 1: BioSign

Global: bases g and h, cryptographic hash function $H(\cdot)$
Input: commitment c, biometric key k, blinding factor γ, payload p
Output: signature σ
$y \leftarrow \mathbb{Z}\,, \quad z \leftarrow \mathbb{Z}$ //draw randomly
$d = g^y \cdot h^z$
$e = H(c, d, p)$
$u = y + e \cdot k, \quad v = z + e \cdot \gamma$
return $\sigma = (d, v, u)$ //pack signature

Generate signature σ for payload p under commitment c with biometric key k and blinding factor γ. Signature σ contains key k only in blinded form.

Algorithm 2: BioVerify

Global: bases g and h, cryptographic hash function $H(\cdot)$
Input: commitment c, signature σ, payload p
Output: *True* or *False*
$(d, v, u) = \sigma$ //unpack signature
$e = H(c, d, p)$
if $g^u \cdot h^v = d \cdot c^e$ **then**
  return *True* //Eq. 3 holds
end
return *False*

Verify signature σ of a payload p using commitment c.

IV. Message Authentication Protocol

The technique we use leverages properties of the integer commitment scheme proposed by Damgard et al. [11]. Each signature is created as a non-interactive proof of knowledge certifying the validity of the biometric measurement provided by the driver. Recipients can verify signatures using an attached commitment. To avoid using a single commitment for multiple messages (which makes them easily attributable to the same sender), our protocol provides OBUs with a set of independent commitments called *bionyms*. Bionyms are indistinguishable from random and cannot be linked. Meaning, a tracking attacker has to re-identify the victim's vehicle every time the OBU switches credentials. This could be protected using an adequate change strategy, e.g., encrypted mix-zones [12]. Randomizing the biometric information also mitigates bionym leakage since it prevents the extraction of the original biometric measurement. This is important as biometric features cannot be changed once revealed to an attacker.

A. Underlying Principle

In order to use Damgard's scheme, a onetime set-up procedure is necessary to determine the public parameters of the scheme. Therefore, the TA constructs an algebraic multiplicative group G such that computing roots of random elements in G is computationally infeasible. The public parameters (g, h) are determined as follows: $h \in G$ is a

randomly picked element and $g = h^{\omega}$ for a random secret ω.[1] The description of G, g, and h are announced to all vehicles in the TA's province and $g \in \langle h \rangle$ is proven without revealing ω via a Schnorr signature based statistical proof of knowledge.

In addition to (g, h), the TA's public key K_{TA}^{+} and the two algorithms BioSign and BioVerify are assumed to be public. These algorithms implement our commitment scheme as shown in Algorithms 1 and 2.

In order for BioSign to authenticate message payload p, three auxiliary inputs are needed: commitment c, biometric key k, and blinding value γ. The signature is generated as described in Algorithm 1 and consists of the tuple $\sigma = (d, v, u)$. What kind of commitment is used by BioSign, depends on the recipient of the message: When interacting with the TA, it is necessary to identify driver D for non-repudiation, hence driver specific commitment C_D is used. When signing an anonymous message, providing a commitment in the form of a bionym b_i is sufficient. b_i contains a random value δ_i to prevent attribution. The commitments and their corresponding blinding factors γ are set as shown in Eq. 1 and 2. In either case, a message's signature σ can be verified as shown in Eq. 3 using BioVerify, if and only if BioSign was invoked with valid inputs.

$$\gamma = s, \qquad c = C_D = g^k \cdot h^s \quad : \text{interacting with TA} \tag{1}$$

$$\gamma = \delta_i + s, \quad c = b_i = C_D \cdot h^{\delta_i} \quad : \text{anonymous messages} \tag{2}$$

$$g^u \cdot h^v = \; g^{y+ek} \cdot h^{z+e\gamma} = g^y \cdot h^z \cdot (g^k \cdot h^{\gamma})^e = d \cdot c^e \tag{3}$$

In the next section, we give a detailed description of the parameters used in the algorithms and explain the three phases of our protocol: *Enrollment*, performed once for every driver, *Bionym Acquisition*, executed periodically when new bionyms are required, and *Message Authentication*, invoked whenever a message is transmitted.

B. Enrollment

Before a vehicle can sign messages under a driver's identity, the driver has to be registered with the TA by providing her identity D, a biometric measurement q, and a secret s stored on a token (see Fig. 3).

An officer at the TA verifies D's identity and ensures that D has provided a genuine biometric measurement q by following the intended acquisition procedure. Afterwards, the biometric key $k = \mathsf{KeyGen}(q)$ is derived. $\mathsf{KeyGen}(\cdot)$ is a key derivation function that transforms the biometric characteristic into a cryptographic secret in an irreversible way similar to a hash function. The resulting secret appears indistinguishable from random and does not allow the inference of any biometric information [13].

After key k is generated, the TA creates an enrollment commitment $C_D = g^k \cdot h^s$ that encapsulates k and thereafter erases s, k, and q. To guarantee that the biometric key cannot be extracted, s is used for blinding. Finally, the driver is notified about the outcome and the tuple (D, C_D) is stored.

When interacting with the TA, the OBU computes C_D on-demand to authenticate as D. Since C_D uniquely identifies a user, it must be encrypted with the TA's public key K_{TA}^{+}. In combination with the random value δ_{seed}, the resulting cipher text changes for every acquisition to prevent identification.

[1] For a detailed description of the parameter initialization, we refer the reader to [11].

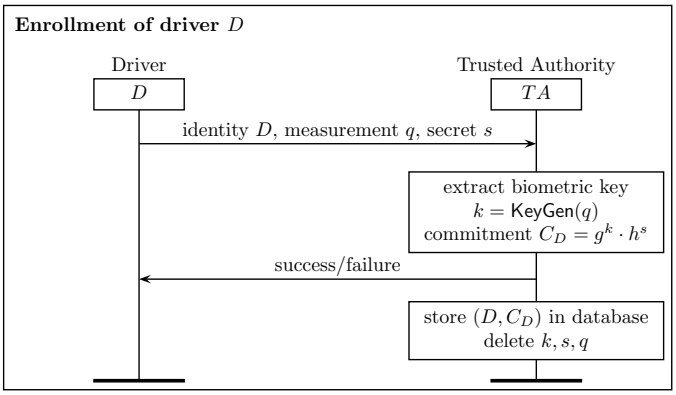

Fig. 3. Enrollment of driver D with the TA. After her identity is confirmed, the enrollment commitment C_D is established.

C. Bionym Acquisition

To send authenticated VANET messages, an OBU has to acquire signing material, i.e., commitments in the form of bionyms. Fig. 4 shows this process starting with the driver providing her secret s and a new biometric measurement q' to the vehicle. In case the driver prevents the acquisition of q', the vehicle will not start if stationary or not be able to participate in the VANET if already driving. After the OBU has extracted the biometric key $k = \mathsf{KeyGen}(q')$, it uses a fresh asymmetric key pair K_V^{-}/K_V^{+} for bionym retrieval. We note that while the biometric has to be provided for each acquisition, s can be stored on the OBU for the duration of the trip. The tuple of public key K_V^{+}, a random seed δ_{seed}, the number of bionyms N, and the driver's identity D form the bionym request r. For authenticity, this request is signed under commitment C_D, key k, and secret s using BioSign. We note that for the generation of N bionyms, N randomization values are needed. To keep the communication overhead small, both entities, OBU and TA expand δ_{seed} to a sequence of N numbers using a cryptographically secure pseudo-random number generator.

Upon receiving an acquisition request, the TA loads the commitment C_D for the claimed identity D and authenticates the request using BioVerify. If successful, δ_{seed} is expanded to the randomization values δ_i to compute the bionyms $b_i = C_D \cdot h^{\delta_i}$ and sign them under the public key K_{TA}^{+}. The TA stores the real identity D with the issued bionyms for non-repudiation. Afterwards, the TA returns the set of bionyms encrypted with the public key provided by the OBU to prevent an attacker from linking the enclosed bionyms. The vehicle verifies the bionyms using its own sequence of randomization values δ_i. The resulting set $\mathbf{B}$ of bionyms and blinding factors γ_i is stored for later use.

D. Message Authentication

The VANET message authentication is depicted in Fig. 5. Analogue to an acquisition request, the biometric key k, a bionym b_i, and blinding factor γ_i are required to sign a message

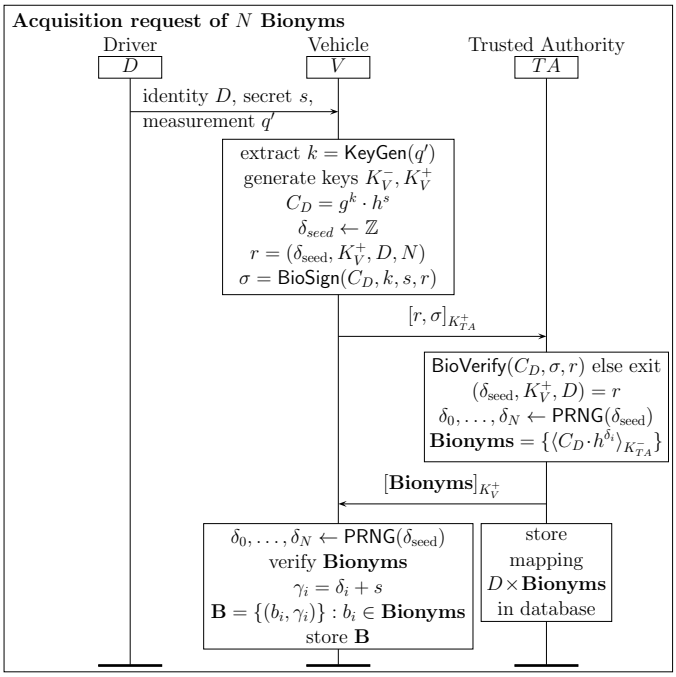

Fig. 4. Acquisition of N bionyms: $[\cdot]_{K_X^+}$ provides encryption and MAC based message integrity, while $\langle \cdot \rangle_{K_X^-}$ provides signatures using asymmetric cryptography with public/private keys of X.

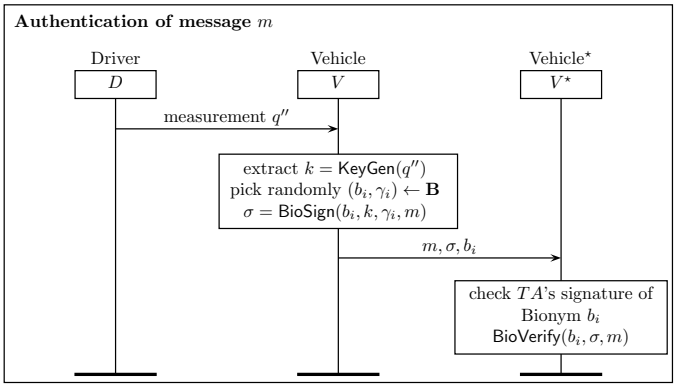

Fig. 5. Authentication of message m: Vehicle V signs m and transmits the message, signature and bionym over the network. Nearby vehicles $V^\star$ validate the bionym and verify the signature.

m. First, a new biometric measurement q'' is acquired from the driver to extract the biometric key k. To prevent linking attacks, the OBU chooses a fresh bionym b_i and the corresponding blinding factor γ_i. Signature σ is computed using BioSign and immediately verified through BioVerify locally. If σ is not valid due to an incorrect k, another biometric measurement is acquired and k regenerated. Finally, the message with signature and bionym is broadcast to nearby vehicles.

Similar to the TA during the bionym acquisition phase, receiving OBUs use BioVerify to check signatures. However, since the sender committed to the bionym at the TA, the bionym's authenticity has to be confirmed using TA's public key K_{TA}^+.

V. Security Analysis

We analyze the resilience against protocol level attacks, which can either be passive eavesdroppers or active manipulators. We assume that the TA's public key K_{TA}^+ is available to all OBUs and has not been compromised.

A. Passive Eavesdropper

The passive adversary uses observed transmissions and tries to compromise secret s, biometric key k, or link consecutive messages of a vehicle for driver tracking and identification.

In general, a driver's secret s is only used in its blinded form $\gamma_i = \delta_i + s$. Therefore, the passive adversary cannot derive any information about its value. The seed δ_{seed} used in a cryptographic pseudo-random number generator to generate the randomization values δ_i is encrypted with K_{TA}^+ and hence protected when transmitted. Further, when overhearing a message, the adversary only learns its signature $\sigma = (d, v, u)$ and bionym b_i. The message m and value d are independent of k and γ_i, and therefore, neither can reveal information about the key or the secret. The values of $u = y + e \cdot k$, $v = z + e \cdot \gamma_i$ and the bionym b_i include k and γ_i in blinded form. Hence, the security of k and γ_i relies on the integer commitment scheme used for signature generation and verification. Damgard et al. [11] show that this scheme is unconditionally hiding under the root assumption. Therefore, any algorithm that could with non-negligible probability extract the biometric key k or γ_i from m, d, v, u and b_i would break the computational Diffie-Hellman assumption.

B. Bionym Linkability

For non-repudiation purposes, the TA can attribute bionyms to drivers using the stored mapping. A passive adversary cannot resolve a bionym directly to an identity. However, he can leverage a bionym's uniqueness in combination with a vehicle's status messages to keep track of its location. As a defense mechanism, an OBU makes use of the fact that they are indistinguishable from random due to the randomization values δ_i and changes bionyms periodically [14]. Bionym acquisitions are also unlinkable, since both the acquisition request and the returned set of certified bionyms are encrypted.

C. Active Manipulation

A Dolev-Yao [15] adversary has full access to the transmission medium, but is not in possession of a victim's secret s or biometric key k. The goal of the adversary is to disseminate messages that are accepted by other vehicles and appear as if they originated from the victim or cannot be attributed to a real identity. We first focus on the case where the adversary replays or forges messages. Then, we analyze an attacker who aims to obtain or forge bionyms.

Message Forging and Replay: When modifying existing or creating new messages, the adversary must make the verifier accept the check $g^u \cdot h^v = d \cdot (b_i)^e$. This means that the signature $\sigma = (d, v, u)$ of message m has to satisfy $d = g^y \cdot h^z$ and $e = H(b_i, d, m)$ which is embedded in v and u. If the adversary cannot create a message that passes the verifier's

check, message authenticity and integrity is fulfilled. According to the hiding property described above, and assuming that $H(\cdot)$ is resistant against second-preimage attacks, an adversary indeed would have to simultaneously guess either k and γ_i or y and z. While k and γ_i can be directly used for signature generation, compromising y and z allows to unblind u and v and obtain values to compute valid signatures. However, the values y, z and γ_i are picked uniformly at random, which means they can only be guessed with negligible probability. The difficulty of guessing k depends on the amount of uncertainty the biometric trait exhibits across a population and how well $\mathsf{KeyGen}(\cdot)$ can extract this entropy. We discuss estimates for this in Section VII.

Neither can the adversary replay an unaltered message, as the ETSI VANET communication standard uses timestamps and sequence numbers as part of the payload for replay protection [14].

Bionym Replenishment: If the adversary attempts to acquire bionyms on a victim's behalf, he has to send his own request to the TA. Signatures for bionym requests are constructed using secret s, commitment C_D and biometric key k; the adversary cannot generate a valid request without those parameters. Moreover, if C_D is unknown, i.e., it has not leaked form the TA, C_D can only be guessed interactively, which can be hardened through rate limiting.

Bionym Forgery: When an adversary $\mathcal{A}$ is denied the acquisition of bionyms because his identity is revoked or not enrolled, he can try to forge bionyms. If the attacker can obtain a victim's biometric measurement q, he can use $\mathsf{KeyGen}(\cdot)$ to extract the biometric key k and choose a random secret s to compute $C_{\mathcal{A}}$. From there, he can construct a bionym $b = C_{\mathcal{A}} \cdot h^{\delta}$ using any δ. Message signatures based on b can be validated with $\mathsf{BioVerify}(\cdot)$, but the attacker cannot sign b with the TA's key K_{TA}^{+} and thus, messages signed with this bionym will be rejected regardless.

VI. Evaluation and Results

We evaluate an implementation of our message authentication scheme by instantiating it with body impedance as the biometric modality. Unlike other biometric methods, that we briefly discuss in Section VII, we argue that body impedance is particularly suited. Driving a vehicle involves holding the steering wheel which can accommodate conductive pads for the unobtrusive acquisition of impedance measurements. Assuming that drivers only infrequently release the steering wheel, measurements can be captured every time whenever both hands touch the pads. The acquisition requires a current smaller than that of a standard battery and is nowhere close to having an effect on the driver's body.

Basic feasibility of body impedance for user authentication and biometric key generation has been shown in the literature [16], [17]. However, since we apply this modality to a scenario not considered so far, where drivers move their hands and occasionally break contact to the conductive pads, we need to test body impedance in a (simulated) driving scenario to review the suitability for our protocol.

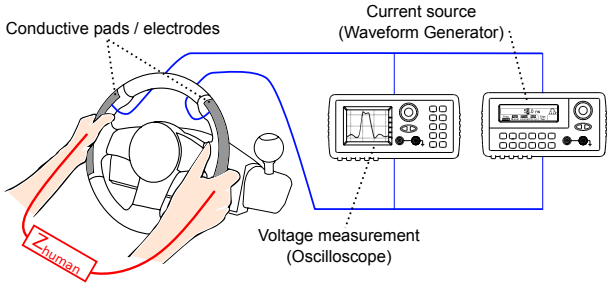

Fig. 6. Measurement set-up: The human subject completes the electric circuit and the body impedance Z_{human} can be acquired.

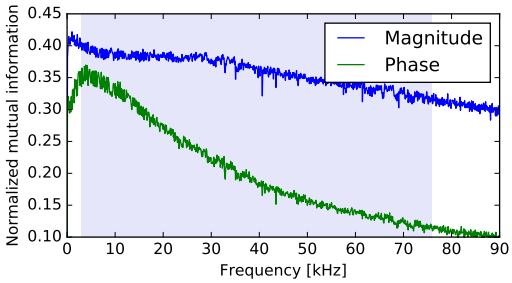

Fig. 7. Normalized mutual information for magnitude and phase of body impedance. Shaded area is the range used for classification.

A. Biometric Performance

Prototype Set-up and User Study: We built a proof-of-concept acquisition system to capture body impedance. A schematic of our set-up is depicted in Fig. 6. Two pads are attached to the sides of an off-the-shelf steering wheel used to control computer games. As soon as the wheel is touched, i.e., short-circuited by a human, one electrode emits a frequency sweep every 3 seconds. These sweeps range from 100 Hz to 100 kHz and are 300 ms long. After the signal has traveled through the human body, it is measured by the second electrode. The emitted signal and the measured signal are then correlated and transformed to the frequency domain in order to compute the complex impedance of the driver.

We conducted a user study with 33 participants (26 male, 7 female). The participants were aged between 25 and 40, and 94% of them owned a driver's license. The ratio between left-hand-side and right-hand-side drivers was 17:14. The participants were asked to sit and hold the steering wheel as if they were in a real car. To eliminate potential bias, the goal of the study was revealed after the fact. We measured the participants' impedance in two configurations: while keeping the wheel still and while controlling a vehicle in a computer game shown on the screen in front of them. For each participant, we acquired 60 measurements over two 4 minute sittings. Having the participants steer a vehicle in first-person view elicits hand movements close to actual driving and the impact of hand positioning and steering motion can be analyzed. On average, participants took 15 left and 12 right turns during their session. 95% of the acquisitions during turning succeeded while 20% of the acquisitions during straight segments failed. Participants were more reluctant to let go of the steering wheel

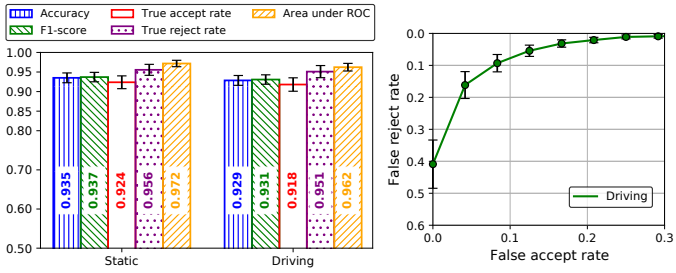

Fig. 8. Body impedance recognition performance for 5 different metrics and receiver operating curve. Results are averaged over the test population and obtained through 5-fold cross-validation. Bars represent 95% confidence intervals.

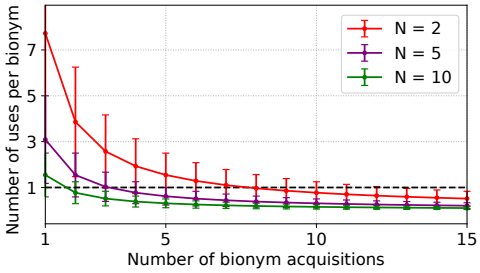

Fig. 9. Communication overhead represented by the number of bionym acquisitions and the associated uses per bionym. Bars represent 95% confidence intervals.

when taking a turn than when driving straight, which explains the difference in acquisition success. Our study was approved by the ethics review board, reference R55051. The voltage level used to acquire the measurements was set to 3 Volts, resulting in a current of 0.2 milli-Amperes, which is far less than what commercially available body fat scales use [18].

Features and Classification: To identify the significant frequencies of the collected impedance measurements, we calculate the normalized mutual information (see Fig. 7). Both, magnitude and phase, are most specific at lower frequencies, letting us choose the complex impedance at frequencies between 2 kHz and 76 kHz as the features for classification. A feature vector extracted from an impedance measurement is the array of its magnitude and phase values. We feed these arrays into a random-forest classifier that decides whether a measurement matches a reference reading of the claimed identity. In total, we train one binary classifier per participant by dividing the samples into two classes. One class comprises all the samples of the participant whose classifier is currently trained and the other class contains all other samples.

Biometric Recognition and Impersonation: We evaluate the performance of biometric recognition based on body impedance using the described set-up. The obtained results determine how likely an enrolled driver is recognized (i.e., bionym request and message authentication are successful), as well as how likely an attacker can impersonate a victim whose secret s has been compromised, that is when the security hinges on the biometric recognition only.

Fig. 8 depicts recognition performance for the configurations *static* and *driving* using 5 different metrics. In order to minimize over-fitting, we conduct 5-fold cross-validation when estimating the metrics. We further ensured that a ratio of 1:1 between measurements of an authorized driver and impersonation attempts was used for both, training and testing, which reduces effects of class imbalance. The values indicate that verification works well; performance for *driving* is on par with *static*. Even though most of the participants stated that they occasionally let go of the steering wheel when they drive their own cars, in our simulation, steering movement and the way drivers hold the wheel affect authentication only marginally. Unless the driver has a completely one-handed driving style, measurements can be captured in rapid succession and compensate for short interruptions. Moreover, as can be seen in the ROC plot in Fig. 8, confidence for the false reject rate is high, implying a low chance for a systematic error. Hence, in a false rejection event due to noisy data or procedure errors, the reading can be re-acquired and is likely to be recognized. Therefore, a higher false reject rate can be tolerated to achieve a lower false accept rate and reduce probability for impersonation.

B. Network Performance

Our scheme implements a refill-based revocation strategy. Every time an OBU attempts to acquire a new batch of N bionyms, the driver can be checked against a revocation list. Once an OBU's storage is depleted and refill is denied, the vehicle will not be able to produce valid message signatures. The duration until revocation comes into effect depends on the number of bionyms released per acquisition and their respective lifetimes. The impact of batch size on communication overhead is evaluated in the following.

Simulation Set-up: We use the simulation of urban mobility [19] (SUMO) for microscopic and continuous road traffic together with the Luxembourg SUMO Traffic (LuST) [20] scenario which provides 24h of vehicle traffic. The road network topology exhibits city properties, i.e. a mesh of small streets interconnected by arterial roads joining a highway tangent to the city. A realistic traffic demand was modeled with two rush hours, one in the morning and one in the evening. The resulting simulation provides a large diversity in trip length, driving speed, and road types that resembles circumstances close to real world traffic. As for the bionym change strategy, we assume a standard compliant fixed bionym change interval [14]. The simulated bionym lifetimes are 50 s, 100 s, and 150 s, in line with literature in [21]. We assume that a vehicle's HSM enforces the bionym life-cycle and runs the protocol as outlined in Section IV.

Bionym Usage: The communication overhead introduced by the acquisition of bionyms is closely coupled with the privacy the signature scheme provides. The frequency of acquisitions determines the availability of bionyms at the OBU and hence its ability to sign messages. In Fig. 9, we highlight the dependency between privacy and communication overhead. In order to prevent (re-)identification of a vehicle by an eavesdropping attacker, a vehicle must not use the same bionym over an

extended period of time. Ideally, a bionym is used for one message only (see horizontal line). We determine the minimum number of acquisitions that satisfy this privacy requirement by simulating the number of uses per bionym for different batch sizes of $N = \{2, 5, 10\}$. Setting the bionym lifetime to 100 seconds, our results show that for 95% of all simulated journeys 12 or more acquisitions are necessary if $N = 2$, versus 2 acquisitions if $N = 10$. Increasing the batch size lowers communication frequency at an increased size per transmission.

VII. Discussion

Continuous Recognition: Other recognition methods that could continuously verify a driver's identity are: face recognition, eye movement tracking [22], driver posture [23], [24], and electrocardiography (ECG) [25]. When using face recognition, special care has to be taken to cope with rapidly changing lighting conditions, e.g., at night time. Furthermore, a camera can record the surroundings and intrude privacy. As for eye tracking, devices are still expensive, require calibration, and are sensitive to changes in lighting and positioning. Research in posture recognition showed a low level of uniqueness among drivers, making it unsuitable for authentication without further refinement. To acquire ECG data, three electrodes have to be placed on the driver, one on each forearm and a reference electrode at the leg, which constrains the range of motion and makes (re-)attaching the electrodes cumbersome.

Biometric Key Generation: Our protocol uses biometric keys instead of a binary decision between accepting and rejecting an identity claim. While our experimental results do not allow to draw conclusions about the difficulty of guessing these biometric keys, they can adequately quantify the probability of impersonation. To obtain an estimate on the strength of keys derived from body impedance, we refer to [17]. In said study, more than 50% of the generated keys exhibit at least 55 bits of entropy and 46 bits on average across a population. The reported false reject rate due to noisy readings is 8.6% and the success rate for impersonation is 1.9%.

VIII. Conclusion

We presented a novel scheme for message authentication in VANETs. Our approach enables the incorporation of biometric measurements into message signatures, transferring the responsibility from vehicle owners to the actual drivers. This provides features not found in existing schemes, such as the exclusion of individuals from the network and the protection of vehicle owners. We offer these guarantees in addition to conditional identity and location privacy of drivers, making the protocol ready for car sharing schemes and TaaS.

In order to assess feasibility of our scheme, we conducted a user study and measured the effect of driver-based credentials on the network. Biometric recognition works sufficiently well and readings are available for signature generation in a timely manner. Although body impedance is particularly suited, the protocol is not limited to the chosen biometric modality. In future work, we expect to assess and compare other biometric methods, such as face recognition, and deploy our message authentication scheme in actual vehicles.

Acknowledgements: This work has been supported by the British Engineering and Physical Sciences Research Council (EPSRC).

References

[1] D. Jiang and L. Delgrossi, "IEEE 802.11p: Towards an international standard for wireless access in vehicular environments," *IEEE Vehicular Technology Conference*, vol. 1, pp. 2036–2040, 2008.

[2] K. Emara *et al.*, "Vehicle Tracking using Vehicular Network Beacons," in *IEEE WoWMoM*, Madrid, Spain, June 2013.

[3] B. Hoh *et al.*, "Achieving guaranteed anonymity in gps traces via uncertainty-aware path cloaking," *IEEE Transactions on Mobile Computing*, vol. 9, pp. 1089–1107, 2010.

[4] M. Khodaei and P. Papadimitratos, "Evaluating On-demand Pseudonym Acquisition Policies in Vehicular Communication Systems," in *ACM IoV/VoI*, Paderborn, Germany, July 2016.

[5] S. Zhao *et al.*, "A survey of applications of identity-based cryptography in mobile ad-hoc networks," *IEEE Communications Surveys Tutorials*, vol. 14, pp. 380–400, 2012.

[6] W. Goodall *et al.*, "The rise of mobility as a service," *Deloitte Rev*, vol. 20, pp. 112–129, 2017.

[7] P. Remyakrishnan and C. Tripti, *A Novel Approach for Enhancing the Security of User Authentication in VANET Using Biometrics*. Berlin, Germany: Springer, 2015, pp. 299–306.

[8] K.-H. Lee and S. K. Kim, "Authentication scheme based on biometric key for vanet information system in m2m application service," *Appl. Math*, vol. 9, pp. 645–651, 2015.

[9] L. Yao *et al.*, "Biometrics-based data link layer anonymous authentication in vanets," in *2013 Seventh International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*. USA: IEEE, 2013, pp. 182–187.

[10] P. Golle and K. Partridge, *On the Anonymity of Home/Work Location Pairs*. Berlin, Germany: Springer, 2009, pp. 390–397.

[11] I. Damgård and E. Fujisaki, "A statistically-hiding integer commitment scheme based on groups with hidden order," in *International Conference on the Theory and Application of Cryptology and Information Security*. Berlin, Germany: Springer, 2002, pp. 125–142.

[12] J. Freudiger *et al.*, "Mix-Zones for Location Privacy in Vehicular Networks," *ACM Workshop on Wireless Networking for Intelligent Transportation Systems (WiN-ITS)*, vol. 51, pp. 1–7, 2007.

[13] C. Rathgeb and A. Uhl, "A survey on biometric cryptosystems and cancelable biometrics," *EURASIP Journal on Information Security*, vol. 10, pp. 1–25, 2011.

[14] ETSI, *Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Definitions*, Jun. 2009.

[15] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Transactions on Information Theory*, vol. 29, pp. 198–208, 1983.

[16] I. Martinovic *et al.*, "Pulse-response: Exploring human body impedance for biometric recognition," *ACM Transactions on Privacy and Security (TOPS)*, vol. 20, p. 6, 2017.

[17] M. Roeschlin *et al.*, "Generating secret keys from biometric body impedance measurements," in *Proceedings of the 2016 ACM Workshop on Privacy in the Electronic Society, WPES@CCS*. New York, NY, USA: ACM, 2016, pp. 59–69.

[18] OMRON Healthcare, "Weight management - frequently asked questions," 2017.

[19] D. Krajzewicz *et al.*, "Recent development and applications of sumo-simulation of urban mobility," *International Journal On Advances in Systems and Measurements*, vol. 5, pp. 128–138, 2012.

[20] L. Codeca *et al.*, "Luxembourg SUMO Traffic (LuST) Scenario: Traffic Demand Evaluation," *IEEE Intelligent Transportation Systems Magazine*, vol. 9, pp. 52–63, 2017.

[21] S. Eichler, "Strategies for Pseudonym Changes in Vehicular Ad Hoc Networks depending on Node Mobility," *2007 IEEE Intelligent Vehicles Symposium*, vol. 5, pp. 541–546, 2007.

[22] S. Eberz *et al.*, "Preventing Lunchtime Attacks: Fighting Insider Threats With Eye Movement Biometrics." *NDSS*, vol. 20, pp. 1–13, 2015.

[23] A. Riener and A. Ferscha, "Supporting implicit human-to-vehicle interaction: Driver identification from sitting postures," in *The first annual international symposium on vehicular computing systems (isvcs 2008)*, vol. 10. USA: isvcs, 2008, p. 10.

[24] T. Kaczmarek *et al.*, "Assentication: User deauthentication and lunchtime attack mitigation with seated posture biometric," *arXiv*, p. 13, 2017.

[25] F. Sufi *et al.*, "Ecg-based authentication," in *Handbook of information and communication security*. Springer, 2010, pp. 309–331.