Noname manuscript No.
(will be inserted by the editor)

Dynamic Attribute Based Vehicle Authentication

Shlomi Dolev · Łukasz Krzywiecki · Nisha Panwar · Michael Segal

Received: date / Accepted: date

Abstract Modern vehicles are proficient in establishing a spontaneous connection over a wireless radio channel, synchronizing actions and information. Security infrastructure is most important in such a sensitive scope of vehicle communication for coordinating actions and avoiding accidents on the road. One of the first security issues that need to be established is authentication via IEEE 1609.2 security infrastructure. According to our preliminary work, vehicle owners are bound to preprocess a certificate from the certificate authority. The certificate carries vehicle static attributes (e.g., licence number, brand and color) certified together with the vehicle public key in a monolithic manner. Nevertheless, a malicious vehicle might clone the static attributes to impersonate a specific vehicle. Therefore, in this paper we consider a sequel attack scenario with multiple malicious vehicles with identical visual static attributes. Apparently, dynamic attributes (e.g., location and direction) can uniquely define a vehicle and can be utilized to resolve the true identity of the vehicle. However, unlike static attributes, dynamic attributes cannot be signed by a trusted authority beforehand. We propose an approach to verify the coupling between non-certified dynamic attributes and certified static attributes on an auxiliary communication channel, for example, a modulated laser beam. Furthermore, we illustrate that the proposed approach can be used to facilitate the usage of existing authentication protocols such as

A preliminary version of this paper has appeared in proceedings of the 13th IEEE International Symposium on Network Computing and Applications (IEEE NCA) 2014 [38].

Shlomi Dolev and Nisha Panwar
Department of Computer Science, Ben-Gurion University of the Negev, Israel.
E-mail: (dolev, panwar)@cs.bgu.ac.il

Łukasz Krzywiecki
Institute of Mathematics and Computer Science, Wrocław University of Technology, Poland.
E-mail: lukasz.krzywiecki@pwr.wroc.pl

Michael Segal
Department of Communication Systems Engineering, Ben-Gurion University of the Negev, Israel.
E-mail: segal@cse.bgu.ac.il

NAXOS, in the new scope of ad-hoc vehicle networks. We use BAN Logic to verify the security claims of the protocol against the passive and active interception.

Keywords Certificate authority · security · vehicle networks · static attributes · dynamic attributes

1 Introduction

Communication security in the scope of vehicle networks [10, 11, 30] introduces new sensitive challenges. A voluntary association among modern vehicles [50] requires a robust authentication mechanism. For example, an instant warning message from a vehicle in front requires an instant authentication before the recipient vehicle reacts according to that warning message. An adversary might influence the origin of a message and might impersonate as an actual sender of the warning message. Apparently, vehicles with identical static attributes might not be authenticated in such a scenario. Currently, the wireless radio communication solely does not support the location binding between the peer communicating partners. It might worsen into a life threatening situation if the adversary is able to fake these warning messages. Moreover, according to the updated traffic rules US Department of Transportation has marked that the inspection authority or police must be able to track and stop any moving vehicle, if it is found to violate the traffic rules [1]. This guideline might require a precise identification of a vehicle, for example in a hit and run case. Therefore, visual sensors and the optical communication channel are used in combination with pre-certified vehicle attributes to ensure a unique visual mapping for each neighboring vehicle.

The goal of this paper is to provide a secure communication over the wireless radio channel through a secure peer-to-peer visual binding over an auxiliary communication channel. The auxiliary communication channel is utilized to create a visual binding and to establish a secure session over the radio channel with the peer vehicle simultaneously visualized over the auxiliary channel. However, the constantly moving vehicles may not be identified solely on the basis of visual static attributes. Therefore, we couple non-certified dynamic attributes (e.g., location and direction) with the certified coupled list of static attributes (e.g., licence number, brand and color) and a public key of the vehicle. Vehicles must verify this coupling between the static and dynamic attributes before the communication begins.

We suggest to use technology assistance, such as laser technology to verify the dynamic attributes. Since dynamic attributes cannot be certified beforehand, we propose to utilize a directional laser beam to bind the dynamic attributes with the monolithically certified coupled static attributes and the public key. Vehicles are required to generate and dispatch the messages from its own laser interface. Therefore, the sender is accountable for any fake message sent and received through its own interface that clearly brings-in a sense of liability in case of any mishappening. Moreover, the corresponding receiver can claim over the sender, which in turn is held responsible and penalized for sending fake messages.

[1] `http://www.jjkellerservices.com/articles/are_you_displaying_right_dot_number.html`

According to our previous work [37], we proposed a modified certificate structure for existing IEEE 1609.2 [1, 2, 4] security standard. The IEEE 1609.2 based security infrastructure provides certificate based authentication. However, we have shown that the naive certificate structure is insufficient to avoid impersonation attacks. In our preliminary work [37], vehicle public key is certified by a Certificate Authority (CA) along with the vehicle static attributes. A certificate recipient must first verify the digital signature over the certificate contents. Second, the coupling between the certified public key and the static attributes must also be verified, in order to authenticate the certificate sender. However, it remains to be shown that *static attribute verification* might not be enough to avoid an impersonation attack for multiple maliciously identical vehicle scenarios.

Problem statement. Vehicles exchange traffic or safety information through a secure wireless radio channel. Every pair of vehicle guarantees the information integrity and the sender authentication through a secure radio channel. However, a peer vehicle cannot visually identify and locate the vehicle in communication. We consider a scenario in which vehicles are allowed to communicate solely over the IEEE 1609.2 enabled 802.11p wireless radio channel. However, the inherent vulnerability of radio communication might impose severe impersonation attacks leading to a strategic crash. We present a scenario with multiple maliciously identical vehicles (further details are given in Section 2). Accordingly, a communicating vehicle is not able to distinguish the authentic vehicle neither through the existing IEEE 1609.2 based PKI settings [2] nor the certified static attribute verification [37]. An adversary might impersonate the visible static attributes of a target vehicle, in spite of being unaware about the secret key of that target vehicle, adversary might be able to create a visual misbinding; hence impersonates to be same as the target vehicle. Consequently, peer vehicles might have an illusion of correct binding with an authentic vehicle around while conveying the warning messages to a malicious vehicle resembling exactly alike. In such a scenario sender vehicle might take some abrupt driving decisions based on a faux-visual and convey these decisions to the following vehicles over a wireless radio channel. However, the visual misbinding might create an illusion to the leading vehicle that the following vehicle has received the warning properly, and is therefore ready to act as per the warning. Apparently, the following vehicle has received the warning on a secure radio session, however, the leading vehicle might not be able to identify this *active recipient* because of the simultaneously existing vehicles that appear exactly alike.

The intended peer vehicle must be verified through some additional means of communication in order to ensure a secure session without any third party interference. Therefore, it is crucial for these vehicles to identify and locate the physical presence of peer vehicles in communication, specifically, in a group of multiple maliciously identical vehicles. The certified coupled static attribute verification might not be enough for this multiple identical vehicle scenario. Therefore, non-certified dynamic attributes must be coupled with the certified static attributes. Firstly, there must be a binding between the certified static attributes and the non-certified dynamic attributes of the vehicle. Secondly, there must be a binding between two communica-

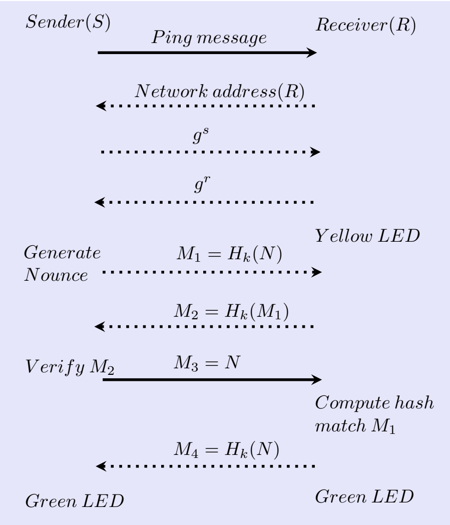


Fig. 1 The approach in [19].

tion channels, i.e., a directed laser beam to convey the certified attributes and a secure wireless radio channel to convey the session messages.

Previous work. In this section, we illustrate the related work, concerning spontaneous wireless vehicle network security threats [13] such as message tampering [42], impersonation [54] and denial of service attack (DoS) [41]. It is important to mention that vehicles utilize wireless communication standard, i.e., IEEE 802.11p Wireless Access in Vehicular Environment (WAVE) based IEEE 1609 Dedicated Short Range Communication (DSRC) [1, 2, 4]. Raya and Haubaux [22, 25, 26] proposed a Public Key Infrastructure (PKI) based vehicle security scheme. The drawback with this approach is that an active adversary may launch an impersonation attack and replace the public key certificate, moreover, roadside infrastructure is required to provide the most updated Certificate Revocation List (CRL). Our scheme eliminates the active impersonation attacks and the participation of roadside units in the authentication process.

State-of-the-art for dual channel association, i.e., wireless radio and out-of-band channel is given in [15]. It is important to mention that the vehicle tracking through the laser beam pointing and scanning is feasible for moving vehicles [35, 36, 40]. Laser communication in vehicular networks has been primarily used for distance and velocity estimation [24, 34]. In [5, 27], laser pointers are used for spontaneous ping among the hand held devices. The work in [23] presents a laser modulation technique to transmit the device network address. However, an adversary can also aim the laser beam with a fake network address and the recipient might not be able to distinguish the authentic laser beam. In [12], the authors suggest the transmission of the shared secret key through the laser modulation. It has the same drawback as with the previous approach [23] that is an adversary equipped with a high resolution camera might

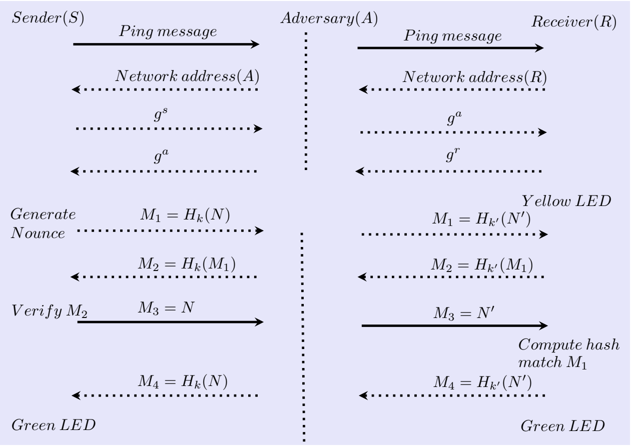


Fig. 2 Man-in-the-middle attack on scheme [19].

capture the laser beam modulation to recover the secret session key. Another work, in [20], presents a visual out-of-band channel. A device can display a two dimensional barcode that encodes the commitment data, hence, a camera equipped device can receive and confirm this commitment data with the available public key. Unfortunately the attacker can still capture and/or fabricate the visible commitment data, as it is not coupled with the public key.

A secure authentication scheme over wireless communication channel is presented in [19]. The scheme utilizes an optical out-of-band communication channel for the *commitment before knowledge* verification while using Diffie-Hellman [9] key exchange on a wireless radio channel beforehand. The idea is to exchange a unique commitment nounce over the optical communication channel instead of a wireless radio channel. However, the optical communication is assumed to be non-confidential and might lead to a subliminal pulse recording. The original detailed approach [19] can be found in our Fig. 1. It must be noticed that an adversary might be active during this key establishment over radio channel. Therefore, sender and receiver establish secret keys with an active adversary in the middle. However, as assumed in their paper the optical laser beam is neither confidential nor one-to-one, therefore, an adversary might encrypt another unique nounce with the secret key and the receiver does not identify the source correctly. The details on this man-in-the-middle attack can be found in Fig. 2. Therefore, this approach is not suitable for vehicle network attack scenarios as the initial key exchange phase on a wireless radio channel is still vulnerable to attack due to the inherently insecure radio communication.

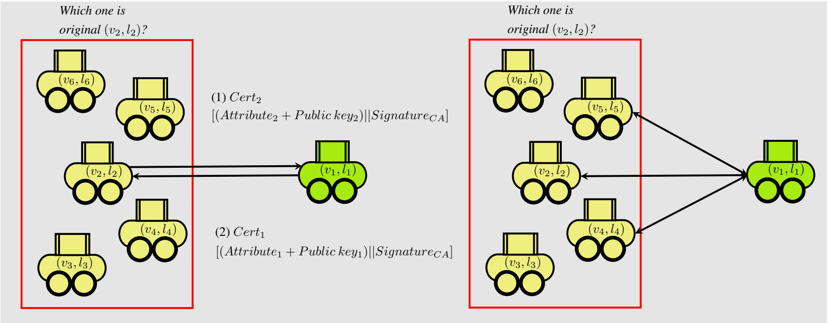
The survey in [21] presents a classification of one-way, two-way and group authentication protocols based on the *commitment before knowledge* principle. The authors in [8] presented an experimental study on visual means of authentication. However, there are no instances of using the laser channel as a means of authentication in vehicular networks and is an important ingredient in our proposed scheme.

Our contribution.

- *Coupling fixed and non-fixed vehicle attributes:* We extend the authentication mechanism within the scope of non-certified dynamic attributes of any vehicle. The proposed approach provides a secure coupling between the fixed and non-fixed attributes via two communication channels, i.e., radio and optical channels, respectively.
- *Optical out-of-band communication channel:* We emphasize that the laser out-of-band communication channel is useful to convey the certified coupled static attributes. It retains the binding between the dynamic and sense-able static attributes of the target vehicle. Vehicles are configured with directed communication capabilities [47], such as laser or directed antenna, used to exchange and verify periodically processed and digitally signed certificates.
- *Adaptation:* The proposed scheme in this paper is versatile and flexible that it can be integrated with the already proven security protocols in order to broaden the security claims required for any specific application. Subsequently, we illustrate a combined security handshake using a main radio and supplementary optical communication channel. Thereby, wlog we highlight the proposed scheme adaptation with NAXOS protocol without weakening the security claims.
- *Verification:* We consider that the real life performance for the proposed approach widely depends on several local factors such as service penetration rate, plausibility, anthropomorphism [43], driver's individual choices. These factors might vary from one region or country to another by great amounts. Therefore, we chose to use the formal method so as to illustrate the extent to which the security claims are being satisfied, i.e., BAN Logic [6]. BAN logic is a predicate based system for conjecture derivation. The protocol idealization and logical deduction results into some pre-defined goals of the security protocol.

The proposed approach is efficient as it completes the certified public key exchange followed by the mutual authentication through visual binding, in two explicit steps (see Fig. 9). Previously existing authentication protocols can be accompanied with the proposed approach without breaching the security claims in the existing security models (e.g., NAXOS adaptation). Furthermore, the proposed authentication protocol is beneficial from channel contention perspective across a crowded junction as it completes in two rounds. Consider an overcrowded road at peak traffic hours during which each vehicle contends for the channel acquisition. The fewer rounds of certificate exchange significantly reduces the authentication overhead for the usage of shared communication band. We detailed a formal verification of the proposed scheme using extended BAN Logic [6,31].

Outline. Section 2 describes a crash scenario and we provide a solution to avoid such a scenario, through the secure visual binding with respect to the auxiliary as well as radio communication channel. The system and hardware settings are given in Section 3. It details the laser characteristics (e.g., range and intensity), applications (e.g., vehicle tracking and speed monitoring), autocollimator setup (e.g., a remote surface angle measurement) and current trends in laser equipped vehicle maneuvering. A detailed description of the proposed approach is given in Section 4. In addition, the section explains the secure binding between the proposed approach and the existing authentication protocol, i.e., NAXOS. Next, a security discussion about the proposed approach is given in Section 5. A detailed proof is given in Section 6 by using an extended BAN Logic formal verification method. Furthermore, Section 7 concludes the discussion on the security of the proposed approach.

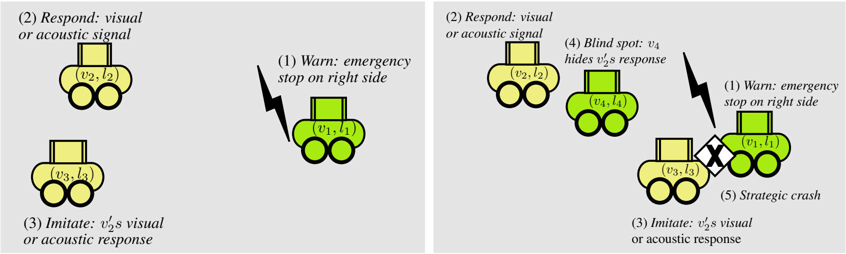

Which one is original (v_2, l_2)?
(v_6, l_6)
(v_5, l_5)
(v_2, l_2)
(v_4, l_4)
(v_3, l_3)
(1) $Cert_2$
$[(Attribute_2 + Public\,key_2)||Signature_{CA}]$
(v_1, l_1)
(2) $Cert_1$
$[(Attribute_1 + Public\,key_1)||Signature_{CA}]$
Which one is original (v_2, l_2)?
(v_6, l_6)
(v_5, l_5)
(v_2, l_2)
(v_4, l_4)
(v_3, l_3)
(v_1, l_1)

Step 1: v_2 sends certificate, $Cert_2$, to v_1. Step 2: v_1 verifies the certificate, $Cert_2$, and responds with the certificate, $Cert_1$, to v_1. Multiple maliciously identical vehicles appear *after* the wireless radio session is secured between v_1 and v_2. Step 3: v_1 cannot distinguish authentic v_2, surrounded by multiple maliciously identical vehicles (on left side). Similarly, v_1 cannot distinguish original v_2 with the authentic and certified static attributes, while group of maliciously identical vehicles appear *before* the wireless radio session is secured between v_1 and v_2 (on right side).

Fig. 3 Multiple maliciously identical vehicles.

2 Attack Scenarios on Static Attribute based Scheme

We propose a novel attack scenario and a verifiable authentication mechanism to avoid these attacks. In [3] vehicle network security and corresponding attacks have been categorized into two such as (1) attacks on the user and (2) attacks on the communication system. Our scenario is based on the former category that endangers the driver safety or provokes the driver himself to undertake any non-safe driving decision that eventually might endanger the safety premises. Moreover, scenarios that harm the user acceptance for the autonomous systems also fall into this category. The later category describes the attack scenario where the communication medium is misused to track the vehicle trajectory or other privacy factors involved therein. The whole protocol construction resides on one-to-one vehicle authentication. It brings into focus two party authentication without any online assistance from controlling authorities, except the pre-processing. In short, our model defines only two roles such as initiator/sender and the correspondingly paired responder/recipient, while avoiding the presence of active impersonation, i.e., man-in-the-middle attack. According to our approach, vehicles may possess a certified list of static attributes and the public key, in order to stipulate a unique identity. However, the *static attribute verification* seems imperfect in a scenario where the adversary encompasses multiple identical vehicles that indeed impersonate a target vehicle, see Fig. 3 and Fig. 4. Vehicles are moving from left to right in all the figures.


(2) *Respond: visual or acoustic signal*
(v_2, l_2)
(1) *Warn: emergency stop on right side*
(v_1, l_1)
(v_3, l_3)
(3) *Imitate: v_2's visual or acoustic response*
(2) *Respond: visual or acoustic signal*
(v_2, l_2)
(4) *Blind spot: v_4 hides v_2's response*
(v_4, l_4)
(1) *Warn: emergency stop on right side*
(v_1, l_1)
(v_3, l_3)
(5) *Strategic crash*
(3) *Imitate: v_2's visual* or acoustic response

Step 1: v_1 warns an emergency stop to v_2. Step 2: v_2 responds with visual or acoustic signal so that v_1 can distinguish it from identical vehicle v_3. Step 3: v_3 imitates every visual or acoustic signal of v_2, to impersonate as v_2 in front of v_1. Step 4: v_4 creates a blind spot and hides the response from v_2. v_1 receives v_3's imitated response, and assumes it to be v_2. Step 5: a strategic crash takes place between v_1 and v_3.

Fig. 4 Strategic crash by maliciously identical vehicles.

Maliciously identical vehicles. A vehicle v_1 can no longer perceive the difference between the communicating partner vehicle v_2 and a group of maliciously identical vehicles around. Multiple identical vehicles appear immediately *after* a vehicle v_1 has established a secret session with v_2, see Fig. 3. Although, v_1 and v_2 are in a secret session, still v_1 cannot identify and locate v_2 among the group of malicious vehicles that carry exactly similar static attributes as v_2 does. A vehicle receives an authentic and certified list of static attributes with the corresponding public key, in order to establish a secret session ensuring information confidentiality. However, a vehicle in an open session with one of the similar looking vehicles, is unable to observe any physical difference. Therefore, the victim vehicle appears to be a member of these malicious vehicles or the other way around that is every identical vehicle seems to be authentic. A similar scenario arises where a group of multiple identical vehicles appear immediately *before* a secret radio session is to be established, on the right side of Fig. 3. Apparently, sender vehicle v_1 visualizes multiple similar vehicles, i.e., v_2, v_4, v_5 on the channel and is forced to select a communicating partner, arbitrarily. As in this case, sender v_2 is able to verify the certified attributes only after sending his own certified attributes and receiving the certified attributes of the specific authentic receiver v_2 in return.

Attack through visual misbinding. In Fig. 4, v_1 establishes a session key with v_2 as only the certified public key of v_2 is coupled with (the sense-able) license number l_2. Apparently, v_3 identifies the existence of communication activity between v_1 and v_2, and subsequently, tries to mimic all out-of-band sense-able behavior of v_2, so that v_1 will not be able to distinguish which one of v_2 and v_3 is v_2. For example, if v_1 requests v_2 to blink over the secured radio channel, v_3 will not be able to decrypt this blink request to v_2. However, v_3 can observe these responses of v_2 and act in the same way by blinking too. It is also important to mention that v_2 cannot identify its own location, in a way that makes it distinguishable from v_3. At this point, v_1 knows that it communicates with the original v_2, but cannot distinguish v_2 from v_3. In addition, consider that v_2 and v_3 are, respectively, on left and right side of the leading vehicle v_1, and v_3's goal is to crash into v_1. If at some point v_1 will perform an emergency stop, then v_1 can notify v_2 on this fact and if lucky stops in the left side of the road in front of v_2. However, v_1 may believe that v_3 is the vehicle it communicate with, v_1 may stop on the right side of the road, allowing v_3 to crash into it.

An adversary might also launch the attack before any session establishment. In that case, multiple maliciously identical vehicles (similar as v_2) appear immediately before the session setup between v_1 and v_2. Consequently, v_1 cannot distinguish between a group of maliciously identical vehicles and the original vehicle v_2.

3 System and Hardware Settings

Today, a connected user experience via wireless radio devices is something we users barely slide off even for the shortest duration [48]. We need to optimize and most importantly secure this capacity of wireless connected shield rising over and above any other recent technology in such a short period. As per our design choices, the combination of an auxiliary optical communication channel and conventional wireless radio channel is feasible and is very much in current trend. In [47] an extended model of radio-over-fiber infrastructure is given, accordingly, a multipoint-to-multipoint connection is the most useful in terms of coverage and capacity. Furthermore, it must be noticed that the laser beam assisted vehicle location binding is secure over the Global Positioning System (GPS) assisted navigation services. The recent paper [49] illustrates the existing and future attack scenarios for GPS spoofing, i.e., fetching wrong location coordinates to the recipient. In the following section we demonstrate the primary hardware settings as is required and feasible in a vehicle network scenario.

Light amplification by stimulated emission of radiation (LASER). Laser is a coherent light beam. It exhibits the spatial and temporal coherence that enables the generation of a narrow light beam over longer distances. Moreover, the data carrying capacity of a laser out-of-band channel is appropriate for the secure data communication.

- It requires less transmission power in a directed/focused light beam over longer distances, e.g., a $0.4 milliradian$ cone may travel up to $300 meter$ to illuminate $1 meter^2$ space.
- It provides more bandwidth and bit carrying capacity, e.g., up to $26 Terabytes$ per second.
- It does not suffer with the frequency interference issues, as the wireless radio signals do.
- It provides a wide detection range with low divergence and high reliability, e.g., up to $1600 meter$ for toward and egress both directions of beam pointing at a specific receiver.
- Laser and radio transmission both travel at the speed of light, still lasers can carry more data at lower power consumption rate, e.g., $1 - 20 Watt$ for the solid state laser beam.
- The laser diode is compact and easy to install, e.g., overall active area is $1/10,000$ of the area used by light emitting diode setup. It can also be aided with fiber optics, hence, the vehicle body weight does not require a redistribution.

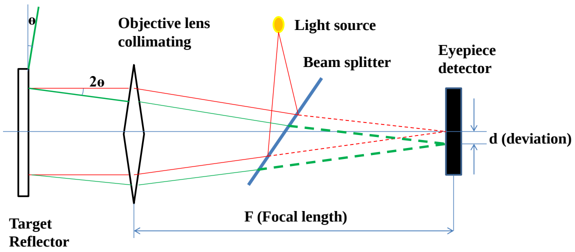


Fig. 5 Laser optoelectronic autocollimator.

- Laser communication cannot be detected with the spectrum analyzer.

On the other hand, laser communication is challenging as it cannot be used in foggy weather and requires a line-of-sight positioning among the communicating nodes.

Light detection and ranging (LIDAR). Mobile laser scanning system can rapidly acquire a 3d-cloud of data points [28], i.e., around 1 million points per second. The spatial coordinates collected by the LIDAR system are processed over additional components such as a digital camera to improve the visualization in real time. In some areas of Europe, LIDAR guns are frequently used by the police for the vehicle tracking. It works on the principle of time-of-flight. It determines the vehicle speed by measuring doppler shift, i.e., the change of wavelength caused by the object movement. If a vehicle A is moving on velocity v_A and the light beam travelling at speed c takes a round trip flight time t_1, then current distance D_1 between the vehicle and the light beam source can be calculated as follows:

$$D_1 = t_1 \times c; D_2 = t_2 \times c \tag{1}$$

For the multiple measurements, in (1), such as flight time t_1, t_2 and distance D_1, D_2 yields the resultant time interval $\Delta t = t_2 - t_1$ and distance traveled $\Delta D = D_2 - D_1$.

$$v_A = \Delta D \div \Delta t \tag{2}$$

Therefore, velocity v_A of vehicle A over the distance ΔD in time Δt can be calculated, see (2) at the source vehicle pointing the laser beam, e.g., a $1KHz$ pulse at $50mW$ for $30ns$ takes $1/250s$ on average to calculate the target speed. However, we emphasize using the laser beam for vehicle identification, i.e., binding the vehicle identity (location) with the physical presence (license number, color).

Autocollimator. We consider that along with the vehicle location tracking, the target surface angle is also a relevant dynamic attribute. Therefore, we assume that vehicles utilize the same laser out-of-band channel for the vehicle location tracking and direction verification. In order to be precise concerning the direction measurements, laser devices are accompanied with the optical autocollimator. Autocollimator eyepiece detector setup never comes into contact with the target object surface. It is most commonly used for the surface parallelism/perpendicularity measurement. There exists

multiple variants of autocollimators such as video (a combination of autocollimator and telescope), visual, digital (optical head with digital controller) and laser beam equipped autocollimators.
Working: It is an optical device that measures the target surface angle using a collimated light beam, see Fig. 5. A collimated light beam is an aligned narrow beam with negligible divergence in the environment, therefore, the beam can travel over larger distances. Light rays start from a light source and reflects from the beam splitter, towards the collimating lens. Collimating lens directs the beam towards the target object. The light rays reflect back from the target object and travel the same path towards the eyepiece detector. If the target object is perpendicular to the horizon, then the reflected light beam intersects at the center of eyepiece detector. Now, the variation in light beam reflection corresponding to the target object angle deviation from the y-axis can be measured, relatively.

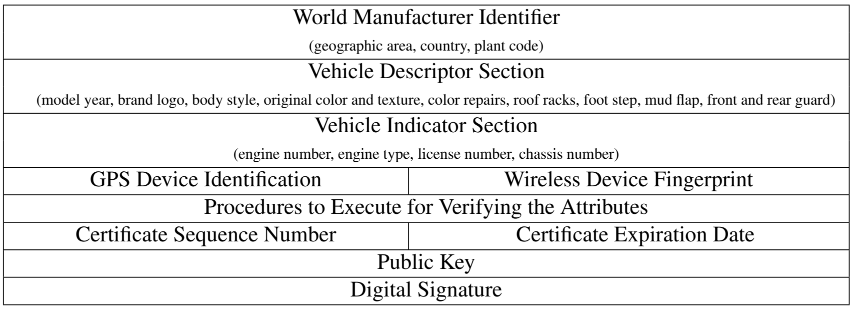
$$d = \varTheta \times f \tag{3}$$

If the target object is tilted at angle $\varTheta$ from y-axis, then the light beam reflects back towards the eyepiece detector at angle $2\varTheta$. This angle $\varTheta$ can be measured through the focal length f of the collimating lens and the light beam deviation d from the center of eyepiece detector, see Equation (3).

Current trends in laser equipped vehicle maneuvering. The laser equipped vehicles are versatile for diverse applications such as driver safety, traffic navigation, vehicle identification, warning dissemination and night vision. The authors in [46] presented a novel approach for the target vehicle information acquisition through a 2d-reflecting code on the front and rear of the vehicle. Accordingly, the infrared laser radar is allowed to scan through the vertical height of the 2d-code pattern at different time intervals. The time sequence based pattern extraction ensures a wider range of code patterns for the different vehicles. Similarly, in [45] a vehicle equipped with inward and outward facing cameras for outside traffic monitoring and driver attention monitoring, respectively, does not provide an overlapped field of view for both cameras. Therefore, the paper presents two laser based calibration methods, namely, coplanar (with internal board pattern and the laser beam) and collinear (with internal and external board pattern as well as the laser beam), that connects the field of view from both cameras. The laser detection and ranging have recently been used for real time parking space locator in [28, 44]. The vehicles capture a 2d-data point collection and derives vehicle size, parking space vacancy and vehicle to vehicle gap. Recently, a major automotive giant has released a laser equipped prototype [32] that increases the night vision effectively. Moreover, it might appear cumbersome to find a suitable place for a moderate size laser device inside the vehicle front without requiring in-vehicle weight re-distribution. Therefore, the usage of fiber optics allows the placement of laser device anywhere within the vehicle, effectively propagating the output to the vehicle front.

4 Dynamic and Static Attributes based Scheme

We aim to verify dynamic attributes along with the monolithically certified static attributes and the public key. The dynamic attribute verification is accomplished through an auxiliary laser communication channel. It is important to mention that a customized certificate structure (see Fig. 6) is used that conveys the certified coupled public key and static attributes, i.e., $Cert = Attribute + PK || Sign_{CA}(Attribute + PK)$. Subsequently, the third round of message exchange over the wireless radio channel is considered implicit. We next list our assumptions as below.



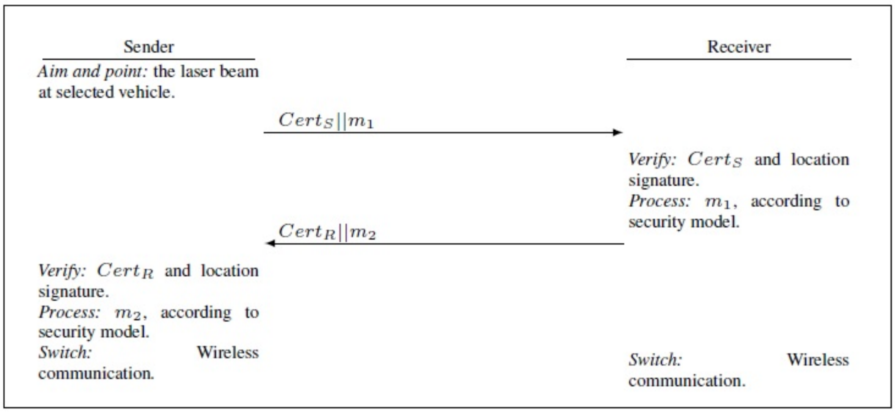
<table>
<tr><td colspan="2">World Manufacturer Identifier
(geographic area, country, plant code)</td></tr>
<tr><td colspan="2">Vehicle Descriptor Section
(model year, brand logo, body style, original color and texture, color repairs, roof racks, foot step, mud flap, front and rear guard)</td></tr>
<tr><td colspan="2">Vehicle Indicator Section
(engine number, engine type, license number, chassis number)</td></tr>
<tr><td>GPS Device Identification</td><td>Wireless Device Fingerprint</td></tr>
<tr><td colspan="2">Procedures to Execute for Verifying the Attributes</td></tr>
<tr><td>Certificate Sequence Number</td><td>Certificate Expiration Date</td></tr>
<tr><td colspan="2">Public Key</td></tr>
<tr><td colspan="2">Digital Signature</td></tr>
</table>

Fig. 6 Certificate structure

Assumptions and mathematical background.

- Vehicles communicate in the presence of PKI that provides periodic certification service.
- Only CA can certify the static attributes and public key using a secret key, however, vehicles can verify those certificate using the corresponding public key of CA.
- Vehicles are equipped with a high precision camera, optical autocollimator, laser beam source and laser beam scanner.
- Considering the problem of view customization and view overlapping for in-built cameras, laser beam is a viable solution [45, 46]. Therefore, it is assumed that a laser beam pointed at the target vehicle cannot be interrupted by the attacker without completely prohibiting the beam to arrive at the target vehicle.
- Vehicles are assumed to be active on a wireless radio channel in order to exchange critical safety warning messages. However, auxiliary communication through a laser beam is utilized for a point-to-point communication where the sender vehicle selects and points a laser beam at the target vehicle. Therefore, sender vehicle utilizes a laser channel in order to create a secure visual binding with respect to a particular target vehicle.

As the presented key agreement protocol and the associated authentication protocols are based on Diffie-Hellman (DH) key exchange. Wlog we assume that corre-



Aim and point: the laser beam at selected vehicle.

Verify: $Cert_S$ and location signature.
Process: m_1, according to security model.

Verify: $Cert_R$ and location signature.
Process: m_2, according to security model.
Switch: Wireless communication.

Switch: Wireless communication.

Fig. 7 The proposed approach.

sponding computations are done within a group $G = \langle g \rangle$ of prime order q, where Computational Diffie-Hellman (CDH) assumption holds.

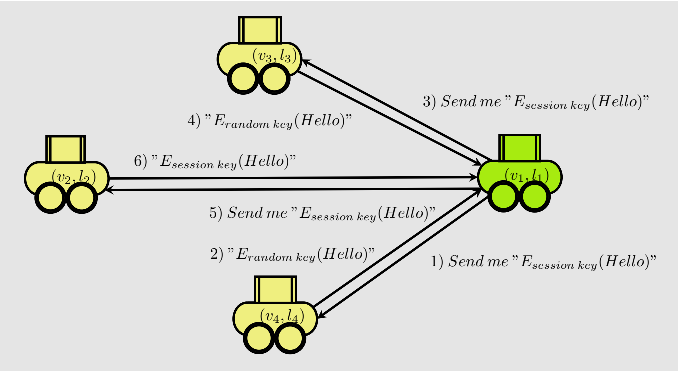
Definition 1 (CDH assumption). *Let $\langle g \rangle$ be a cyclic group generated by element g of order q. There is no efficient probabilistic algorithm $\mathcal{A}_{CDH}$ that given $(g, g^{\alpha}, g^{\beta})$ produces $g^{\alpha\beta}$, where α, β are chosen at random from G.*

The CDH assumption satisfies that the computation of a discrete logarithm function DL on public values $(g, g^{\alpha}, g^{\beta})$ is hard [18] within the cyclic group G.

Proposed approach. In Fig. 7, a generalized form of the proposed authentication protocol has been shown. Each round includes the transmission of a customized certificate along with the authentication message. Accordingly, in the first round, sender

S	Sender	R	Receiver
$Cert_S$	Certificate of sender	$Cert_R$	Certificate of receiver
PK_{CA}	Public key of CA	SK_{CA}	Secret key of CA
PK_S	Public key of S	PK_R	Public key of R
SK_S	Secret key of S	SK_R	Secret key of R
eSK_S	Ephemeral secret key of S	eSK_R	Ephemeral secret key of R
$Attribute_S$	Static attributes of S	$Attribute_R$	Static attributes of R
SN_S	Sequence number of S	SN_R	Sequence number of R
H	Hash function	K	Session key
X	$g^{H_1(eSK_S,SK_S)}$ from S	Y	$g^{H_1(eSK_R,SK_R)}$ from R
H_1	Hashing function for X and Y	H_2	Hashing function for session key K
E_{PK}	Encryption with the public key	D_{PK}	Decryption with the public key
E_{SK}	Encryption with the secret key	D_{SK}	Decryption with the secret key
v	Vehicle	l	License number

Table 1 Notations.


(v_3, l_3)
3) $Send\, me$ "$E_{session\ key}(Hello)$"
4) "$E_{random\ key}(Hello)$"
6) "$E_{session\ key}(Hello)$"
(v_2, l_2)
(v_1, l_1)
5) $Send\, me$ "$E_{session\ key}(Hello)$"
2) "$E_{random\ key}(Hello)$"
1) $Send\, me$ "$E_{session\ key}(Hello)$"
(v_4, l_4)

Step 1: v_1 requests for session key encrypted message, $E_{session\ key}(Hello)$, to v_4. Step 2: v_4 with a random key encrypted message, $E_{random\ key}(Hello)$, to v_1. v_1 declines v_4 authentication. Step 3: v_1 requests for session key encrypted message, $E_{session\ key}(Hello)$, to v_3. Step 4: v_3 responds with a random key encrypted message, $E_{random\ key}(Hello)$, to v_1. v_1 declines v_3 authentication. Step 5: v_1 requests for session key encrypted message, $E_{session\ key}(Hello)$, to v_2. Step 6: v_2 responds with a session key encrypted message, $E_{session\ key}(Hello)$, to v_1. v_1 validates the v_2's re-authenticates, after verifying the current session key.

Fig. 8 Re-authentication.

vehicle selects a vehicle for communication and points the laser beam. The sender forwards its own certificate $Cert_S$ over the laser channel. At this point the customized certificate structure is accompanied with an authentication message. The authentication message from the sender, i.e., m_1 is received and processed as per the associated security model. The receiver verifies the binding between certificate $Cert_S$ and the message m_1 followed by the binding between certified static attributes and the physical location of the vehicle. Now, the message m_1 is recovered and used to compute the session key at receiver. Similarly, the receiver forwards its own certificate $Cert_R$ accompanied with the authentication message m_2 over laser channel. The sender verifies the attribute binding with the public key and processes the message m_2 as per the associated security model.

We utilize laser out-of-band communication channel for both the certified and non-certified attribute verification concurrently. Vehicle v_S starts the communication on a modulated laser communication channel by aiming and pointing the laser beam on target recipient v_R. Once the master session key is computed, both vehicles switch on to wireless radio communication and use symmetric encryption over the wireless radio channel. The receiver must create a binding between the certified attributes received on the laser communication channel and the dynamic attributes recovered from the laser beam. All notations are given in Table 4.

In our scheme v_S can identify v_R among the group of maliciously identical vehicles (similar as v_2), see Fig. 8. Vehicle v_S might visualize multiple identical vehicles, but is already in a secret session with v_R. Therefore, to accomplish the *re-authentication*, v_S starts pointing laser beam at each of these identical vehicles, because only one of these identical vehicles must respond through a correct session key encryption. It points a laser beam on a suspect vehicle and requests a session key

1. Sender aims and points the laser beam at the selected vehicle, in order to convey the certified coupled public key and the static attributes.
2. Sender computes the ephemeral secret key eSK_S and then the secret hashed exponent $H_1(eSK_S, SK_S)$.
3. Sender S sends the signed certificate with message X, i.e., $Cert_S||X$. Where X is $g^{H_1(eSK_S,SK_S)}$.
4. Receiver R:
   (a) Verifies the digital signature using the CA public key PK_{CA}.
   (b) Verifies the binding between the visual static attributes $Attribute_S$ and the location using out-of-band channels, i.e., thermal image camera and laser based autocollimator, respectively.
   (c) Computes the ephemeral secret key eSK_R and the exponent $H_1(eSK_R, SK_R)$. In addition, computes the secret session key K, i.e., $H_2(PK_S^{H_1(eSK_R,SK_R)}, X^{SK_R}, X^{H_1(eSK_R,SK_R)}, S, R)$.
   (d) Responds with the signed certificate $Cert_R||E_{PK_S}(E_{SK_R}(Y + SN_S))$. Consider Y as $g^{H_1(eSK_R,SK_R)}$, also concatenated with the certificate sequence number SN_S and signed with the PK_S and SK_R.
5. Sender S:
   (a) Verifies the digital signature using the CA public key PK_{CA}.
   (b) Verifies the binding between the visual static attributes $Attribute_R$ and the location using out-of-band channels, i.e., thermal image camera and laser based autocollimator, respectively.
   (c) Decrypts the value Y and the concatenated certificate sequence number SN_S, i.e., $D_{SK_S}(D_{PK_R}(Y + SN_S))$. In addition, computes the secret session key K, i.e., $H_2(Y^{SK_S}, PK_R^{H_1(eSK_S,SK_S)}, Y^{H_1(eSK_S,SK_S)}, S, R)$.
6. Sender and receiver exchange the session messages encrypted with the session key K.

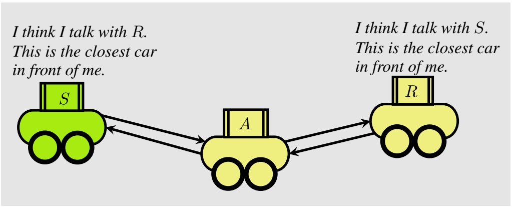
Fig. 9 Adaptation with NAXOS protocol.

encrypted response. Now, if the suspect vehicle is the original vehicle v_R that was already in an open secret session before the group of malicious vehicle appeared, than it must respond to v_S with a correct session key encryption. Apparently, v_S can locate the vehicle on which it aims and points the laser beam. Therefore, after v_S receives the correct session key encrypted response from v_R, it stops the *re-authentication* for the remaining identical vehicles, and follows the trajectory of v_R for the rest of the session.

Binding with the Existing Protocol Our approach provides a straight binding between the vehicle locations, certified static attributes and the public key. It is important to mention that our protocol can be combined with the well known existing authentication protocols, e.g., SIGMA [14], NAXOS [16], NAXOS+ [17], CMQV [33], SMQV [29] already proven to be secure in existing models such as CK [7], eCK [16] and seCK [29]. In that case message m_1 and m_2 can be computed with any one of these authentication protocols at sender and receiver, independently.

Our paper illustrates the secure binding between the optical and wireless communication channel rather the security of existing authentication protocols, i.e., SIGMA, NAXOS and NAXOS+. Therefore, the interested readers may refer to the proven security features of these authentication protocols in the extended security models. Furthermore, wlog we combine the proposed approach with the NAXOS, in order to illustrate the vehicle authentication. NAXOS assumes that sender and receiver have already exchanged the public key/certificate and requires additional two rounds for the ephemeral key exchange and session key establishment. NAXOS is resistant to the following attacks, where adversary recovers:

- *Key-Compromise Impersonation*
  - the long-term secret key of S, still cannot impersonate others to S.


I think I talk with R.
This is the closest car in front of me.
S
A
I think I talk with S.
This is the closest car in front of me.
R

In this Fig., adversary A carries same static attributes as R and impersonates as R in front of S.

Fig. 10 Misbinding scenario.

  - the ephemeral secret key of S, still cannot impersonate others to S.
- *Session Key Retrieval*
  - the ephemeral secret key of both parties, still cannot derive the session key.
  - the long term secret key of one party and the ephemeral secret key of another party, still cannot derive the session key.
  - the long term secret key of both parties, still cannot derive the session key.

NAXOS protocol assumes that the public key has been exchanged in secure settings and requires an additional two rounds to establish a secret session key among the parties. Apparently, this is not the case in our protocol, here it requires two explicit rounds of certificate exchange and session key establishment, without any previous identity or public key exchange. Our generalized solution merges the multiple rounds into two, see Fig. 9. However, the proposed protocol benefits from the existing secure authentication protocols, in addition, provides a certified visual binding and does not interfere with the security claims of associated authentication protocol.

5 Security Discussion

In this section, we analyse the security of the proposed approach against an active and passive attack scenario.

Passive adversary. The proposed approach is secure against the passive eavesdropping over the channel. The sender and receiver establish a laser communication channel, which is characterized by a *directed point-to-point* connection. Due to the physical constraints of this auxiliary authentication channel, passive listening is not possible. Passive eavesdropping on the laser channel will prohibit the data transmission between the sender and receiver, as it necessitates a line-of-sight for the beam pointing. Any kind of obstruction between the vehicles will absorb the light beam. Hence, no passive adversary can overhear the messages on a laser beam without stopping the beam to reach the intended recipient.

Active adversary. An active impersonation, see Fig. 10, allows the adversary to *intercept, remove, skip, delay, manipulate* or *insert fake* messages, in a *man-in-the-middle* manner. Here, we assume that the adversary is equipped with the double laser interfaces (e.g., in front, and at the back of the car). Therefore, it can receive the messages from the intended sender's front interface towards its back interface. The active adversary forwards the same messages to the intended receiver's back interface, using its own front interface. Similarly, it forwards the response messages from the intended receiver (in front) towards the intended sender (behind). Now, the active adversary can launch an active attack in either of the following two ways:

- The active adversary with exact *matching static attributes* tries to *intercept, remove,* and *skip* or *delay* the messages between the intended sender and receiver. The active adversary does not modify the messages and its goal is to convince the sender and the receiver that they communicate with the intended car, i.e., visually identified. The active adversary has exact similar static attributes as the intended recipient carries in order to impersonate the recipient. However, vehicles receive certified attributes, which are then visually verified before the processing of messages of the accompanying authentication protocol. Therefore, to act as a forwarder, the proxy adversary should look like the sender in front of the receiver and the intended receiver in front of the sender (both at the same time), in order to qualify the attribute verification on both sides. This if not impossible still is very unlikely, and can be disregarded for the current system settings. Although, we extend the message forwarding attack scenario in another work [39].
- The active adversary tries to *manipulate* or *insert fake* messages. The intended sender and receiver exchange the messages with a false impression that they communicate directly to each other. Whereas, the active adversary with exact *matching static attributes* sits in the middle and either modifies or injects fake message to each other, correspondingly. However, our approach guarantees to resolve the vehicle identity in the presence of multiple identical vehicles. Furthermore, the binding between augmented certificate and laser communication channel does not weaken the security of the associated authentication protocol, such as NAXOS, which has proven to be secure in an extended model.

Protocols	**Iteration cost**	**Exponentiation**	**Credentials**	**Property**
Proposed	2	1	CDH+OOB	Identity binding +AKE
SIGMA [14]	3	2	DH	Anonymity+AKE
NAXOS [16]	3	4	GDH	KCI+wPFS+AKE
NAXOS+ [17]	3	5	CDH	KCI+wPFS+AKE

Table 2 Performance evaluation.

Furthermore, a performance comparison regarding the proposed approach and the existing protocols is given in Table 2. Accordingly, the first criteria of comparison is the *iteration cost* that determines the communication complexity. The proposed approach requires only two rounds of radio communication, i.e., sender-to-receiver and receiver-to-sender, as a part of authenticated key exchange. Another primitive is *exponentiation* that determines the computation complexity based on atomic operations. Evidently, the proposed approach requires only the recipient to compute single exponentiation for a complete execution of the protocol initiated by the sender. However, this reduction in the number of exponentiations must be compensated with the supplementary out-of-band verification OOB. The *credential* security relies on the underlying assumptions of the DH and OOB verification. In addition, the proposed approach satisfy *properties*, i.e., secure identity binding and the authenticated key exchange.

6 Security Analysis using BAN Logic

In this section, we illustrate the security analysis using BAN Logic [6] and the PKI based extended BAN Logic [31]. First, we use the basic terminology and inference rules of BAN Logic. Next, a formal protocol interpretation, initial assumptions, protocol analysis goals and logic derivation is introduced for the proposed protocol. The BAN Logic is chosen over other verification methods to provide a higher order logic abstraction. It derives a tight logical reduction of pre-assumed annotations into expected security goals and provides less complex adversary trace analysis.

BAN Logic presents a highly expressive logical notion of authentication protocols [51–53]. Entities in communication visualize and interact through message exchange. It is enriched with security primitives such as encryption, decryption, signcryption and PKI based certificate authentication. It provides logical postulates that can be combined with the formal protocol idealization phase. Every transition from any message exchange leads to a certain logical premise where these postulates such as message meaning rules, nonce verification rules, jurisdiction rules and universal or existential quantification; are applicable in a certain sequence. A tight reduction from pre-defined assumption towards the analysis goals of the protocol allows a successful verification of security properties. A formal protocol interpretation requires formal initial assumptions, analysis goals, annotations, logical inferences. For example, if Bs prospective is that A deduced the message m and that message m is recent on the channel then B must also believe that A sent message m on the channel.

Basic notations. The BAN Logic notations shown below are used to derive and analyze the protocol assumptions and goals.

$$\begin{aligned}
S \mid\equiv X &: S\, believes\, X;\\
S \lhd X &: S\, sees\, X;\\
S \mid\sim X &: S\, said\, X;\\
S \Rightarrow X &: S\, controls\, X;\\
\sharp(X) &: X \text{ is } fresh;\\
S \xleftrightarrow{K_{SR}} R &: S \text{ and } R \text{ share a secret key } K_{SR};\\
X_{K_{SR}} &: X \text{ encrypted with } K_{SR};\\
\wp\kappa(S, K_S) &: S \text{ has public key } K_S;\\
\prod(S, K_S^{-1}) &: S \text{ has secret key } K_S^{-1};\\
\sigma(X, K_S^{-1}) &: X \text{ signed with private key } K_S^{-1};\\
S \rightarrow R :\ (X, \Re(X, R)) &: S \text{ sends } X \text{ to the intended recepient } R;\\
\sigma(\Re(X, S), K_R^{-1}) &: X \text{ signed with private key } K_R^{-1} \text{ for } S;\\
\{\varsigma(X, R)\}_{K_S} &: X \text{ signed with public key } K_S \text{ from } R.
\end{aligned}$$

Logical inferences. There exist some pre-determined logical postulates as follows. These inferences can be used together with the protocol assumptions (in next subsection) to attain the protocol analysis goals.
Message meaning rule: It concerns with the origin of encrypted messages. If S believes in CA's public key K_{CA} and private key K_{CA}^{-1}, and S see the message encrypted with K_{CA}^{-1} from the intended sender R, then S believes that the CA generated this message.

$$\frac{S \mid\equiv \wp\kappa(CA, K_{CA}), S \mid\equiv \prod(CA, K_{CA}^{-1}), S \lhd (\varsigma\{X, CA\}_{K_{CA}^{-1}})}{S \mid\equiv CA \mid\sim X} \tag{4}$$

S believes in public key K_R and private key K_R^{-1}, and see the message encrypted with private key K_R^{-1} for which S is the intended recipient, then S believes that R said X.

$$\frac{S \mid\equiv \wp\kappa(R, K_R), S \mid\equiv \prod(R, K_R^{-1}), S \lhd \sigma(\Re(X, S), K_R^{-1})}{S \mid\equiv R \mid\sim X} \tag{5}$$

S believes in a certificate from CA. If S believes that CA believes in the validity duration t of the certificate and and credential $\varPhi(st)$ is still valid, then S believes that CA believed in the statement st for the duration t.

$$\frac{S \mid\equiv CA \mid\sim (Cert(t, st)), S \mid\equiv CA \mid\equiv t, S \mid\equiv CA \mid\equiv \varPhi(st)}{S \mid\equiv CA \mid\equiv st} \tag{6}$$

Nonce verification rule: This rule concerns with the validity of messages with respect to time. If S believes that a message X is fresh and that R said the message X, then S believes that R believes in the freshness of X.

$$\frac{S \mid\equiv \sharp(X), S \mid\equiv R \mid\sim X}{S \mid\equiv R \mid\equiv X} \tag{7}$$

Jurisdiction rule: If S believes that R controls the message X and also believes in the message X, then S believes in the message X.

$$\frac{S \mid\equiv R \Rightarrow X, S \mid\equiv R \mid\equiv X}{S \mid\equiv X} \tag{8}$$

Decomposition rules: It concerns that if a message is partly fresh then whole message is fresh. Similarly, if a message can be decrypted then its components are also decrypted. For the last rule if S can see a signed message X intended for all then S is also one of the intended recipient for the message X.

$$\frac{S \mid\equiv \sharp(X)}{S \mid\equiv \sharp(X, Y)}, \frac{S \lhd (X, Y)}{S \lhd X}, \frac{S \lhd \sigma(\Re(X, all), K_{CA}^{-1})}{S \lhd \sigma(\Re(X, S), K_{CA}^{-1})} \tag{9}$$

Quantifiers: Above stated rules can be augmented with the implicit or explicit quantifiers, as per the assumptions. For example, in the following postulate we assume a universal quantification, where S believes that CA controls the shared key K between S and R.

$$S \mid\equiv CA \Rightarrow S \overset{K}{\longleftrightarrow} R$$

While it can also be augmented, explicitly, as follows

$$S \mid\equiv \forall K (CA \Rightarrow S \overset{K}{\longleftrightarrow} R)$$

Protocol Idealization. The two round protocol using the binding between auxiliary laser channel and certified static attributes at are formalized as below. In this idealization $Cert_x(t, st)$ represents the certificate with a validity duration t and the credential statement st (coupled attributes and the public key), which is valid only for the duration t.

$$\begin{aligned} Cert_x(t, st) &= \sigma(\Re((at_x + K_x), \prod(K_x^{-1}), all), K_{CA}^{-1}) \\ \sigma(Cert_x, K_{CA}^{-1}) &= at_x + K_x || Sign_{CA}(at_x + K_x) \end{aligned} \tag{10}$$

The message M_1. carries $Cert_S||m_1$ from sender to receiver.

$$\begin{aligned} \mathbf{M}_1 &: S \rightarrow R : Cert_S || m_1 \\ &: \{at_S + K_S || Sign_{CA}(at_S + K_S)\} || E_{K_S^{-1}}(g^{\alpha}) \end{aligned} \tag{11}$$

Similarly, M_2. represents the response $Cert_R||m_2$ from receiver to sender.

$$\begin{aligned} \mathbf{M}_2 &: R \rightarrow S : Cert_R || m_2 \\ &: \{at_R + K_R || Sign_{CA}(at_R + K_R)\} || E_{K_S}(E_{K_R^{-1}}(g^{\beta} + SN_S)) \end{aligned} \tag{12}$$

Initial assumptions. According to the protocol every vehicle is installed with the signed certificates from CA. Therefore, the sender S and receiver R have some predetermined belief in associated public/private key pairs. These beliefs can be summarized as below:

$$\begin{array}{lllll}
A1 & : S & \mid\equiv & \wp\kappa(CA, K_{CA}) & S \text{ believes } CA \text{ has a public key } K_{CA}; \\
A2 & : S & \mid\equiv & \prod(K_{CA}^{-1}) & S \text{ believes } CA \text{ has a private key } K_{CA}^{-1}; \\
A3 & : R & \mid\equiv & \wp\kappa(CA, K_{CA}) & R \text{ believes } CA \text{ has a public key } K_{CA}; \\
A4 & : R & \mid\equiv & \prod(K_{CA}^{-1}) & R \text{ believes } CA \text{ has a private key } K_{CA}^{-1}; \\
A5 & : S & \mid\equiv & \wp\kappa(S, K_S) & S \text{ believes } S \text{ has a public key } K_S; \\
A6 & : S & \mid\equiv & \prod(K^{-1}{}_S) & S \text{ believes } S \text{ has a private key } K^{-1}{}_S; \\
A7 & : S & \mid\equiv & Cert_S(t, st) & S \text{ believes in certificate } Cert_S; \\
A8 & : R & \mid\equiv & \wp\kappa(R, K_R) & R \text{ believes } R \text{ has a public key } K_R; \\
A9 & : R & \mid\equiv & \prod(K_R^{-1}) & R \text{ believes } R \text{ has a private key } K_R^{-1}; \\
A10 & : R & \mid\equiv & Cert_R(t, st) & R \text{ believes in certificate } Cert_R; \\
A11 & : S & \mid\equiv & \forall x \, CA \Rightarrow Cert_x & S \text{ believes } CA \text{ controls certificate;} \\
A12 & : R & \mid\equiv & \forall x \, CA \Rightarrow Cert_x & R \text{ believes } CA \text{ controls certificate.}
\end{array}$$

Analysis goals. We illustrate the protocol analysis goals below. It would be useful to interpret the claims regarding active and passive adversary. Goal $G1$ and $G2$ can be interpreted as the belief in public key signed by CA. Every vehicle believes in his own public/private key pair, however, to receive the correct public key from the sender over the insecure channel, receiver must acquire a confidence in the certificate credentials. Therefore, first two goals are devoted to stipulate that both the parties R and S believes in the correct public key that is K_S and K_R, respectively.

$$\begin{aligned} G1: &\quad R \mid\equiv \sigma(K_S, K_{CA}^{-1}); \\ G2: &\quad S \mid\equiv \sigma(K_R, K_{CA}^{-1}); \end{aligned}$$

Other two goals $G3$ and $G4$ can be deduced as R believes in $Cert_S||m_1$ from the intended sender S and similarly, S believes that it is the intended recipient for $Cert_R||m_2$.

$$\begin{aligned} G3: &\quad R \mid\equiv \varsigma(Cert_S(t, st)||m_1, S); \\ G4: &\quad S \mid\equiv \Re(Cert_R(t, st)||m_2, S). \end{aligned}$$

Logic derivation. We drive the first order belief for the corresponding sender and receiver in both rounds. The first round, sender S forwards a signed certificate to the receiver R. In addition, R can decrypt and verify the messages signed by the CA. The recipient R believes in the message signed by the CA, see (10). By applying $A3$ and $A4$ with the *Message meaning rule* given in (4), R believes that CA said $Cert_S(t, st)$.

$$\frac{R \mid\equiv \wp\kappa(CA, K_{CA}), R \mid\equiv \prod(CA, K_{CA}^{-1}), R \triangleleft (\varsigma\{Cert_S(t, st), S\}_{K_{CA}^{-1}})}{R \mid\equiv CA \mid\sim Cert_S(t, st)}$$

Hence, R believes that the certificate has been originated at CA. Now, applying the *Message meaning rule* given in (6) as follows.

$$\frac{R \mid\equiv CA \mid\sim (Cert_S(t, st)), R \mid\equiv CA \mid\equiv t, R \mid\equiv CA \mid\equiv \varPhi(st)}{R \mid\equiv CA \mid\equiv st} \tag{13}$$

As per (13), R believes that CA believes in the certificate credential, i.e., *st*. It yields a second order belief that CA believes in $cert_S$. Now applying (13) with the first *Decomposition rule* given in (9).

$$\frac{CA \mid\equiv \sharp(st)}{CA \mid\equiv \sharp(Cert_S(t, st))} \tag{14}$$

Hence, using *Jurisdiction rule* given in (8) with the derivation in (13) with the assumption in $A12$. The following equation yields a first order belief that R believes in $Cert_S$.

$$\frac{R \mid\equiv CA \Rightarrow Cert_S(t, st), R \mid\equiv CA \mid\equiv Cert_S(t, st)}{R \mid\equiv Cert_S(t, st)} \tag{15}$$

Therefore, R believes in the $Cert_S$ and that S associates a good public/private key pair, thereby satisfies the goal $G1$.

$$\frac{R \mid\equiv \wp\kappa(S, K_S), R \mid\equiv \prod(S, K_S^{-1}), R \triangleleft \sigma(\Re(m_1, R), K_S^{-1})}{R \mid\equiv S \mid\sim m_1} \tag{16}$$

According to (16), R receives m_1 along with the certificate st. While, m_1 is encrypted with the private key K_S^{-1}. Therefore, R infers that S said m_1. It is important to mention that the receiver R follows the decomposition rule in (9), in order to infer the intended recipient for the secret key K_S^{-1} encrypted message m_1. Now, combining (16) with the first order and second order belief derived in (15) and (14), respectively. Hence, satisfies the goal $G3$.

$$\begin{aligned} M_1 \ &: R \mid\equiv CA \mid\equiv Cert_S(t, st) \\ &: R \mid\equiv Cert_S(t, st) \text{ and } R \mid\equiv S \mid\sim m_1 \\ &: R \mid\equiv (\varsigma(m_1, S), K_{CA}^{-1}) \end{aligned} \tag{17}$$

Consequently, for the message M_2. in second round, S verifies the certificate signature in $Cert_R$. By applying the assumptions $A1,\ A2,\ A5,\ A6$ with the *Message meaning rule* given in (4), S believes that the CA said $Cert_R(t, st)$.

$$\frac{S \mid\equiv \wp\kappa(CA, K_{CA}), S \mid\equiv \prod(CA, K_{CA}^{-1}), S \triangleleft (\varsigma\{Cert_R(t, st), R\}_{K_{CA}^{-1}})}{S \mid\equiv CA \mid\sim Cert_R(t, st)}$$

Now, applying the *Message meaning rule* in (6), S believes that the CA believes in the *st* from R. Apparently, second order belief is accomplished in (18).

$$\frac{S \mid\equiv CA \mid\sim (Cert_R(t, st)), S \mid\equiv CA \mid\equiv \Delta t, S \mid\equiv CA \mid\equiv \Phi(st)}{S \mid\equiv CA \mid\equiv st} \tag{18}$$

Next, the *Decomposition rule* given in (9) is combined with (18). It derives that if CA believes in *st* then it also believes in the $Cert_R$ as follows.

$$\frac{CA \mid\equiv \sharp(st)}{CA \mid\equiv \sharp(Cert_S(t, st))} \tag{19}$$

Applying *Jurisdiction rule* given in (8) with the current (19) and assumption $A11$. Now, S also believes in the $Cert_R$. The following equation yields a first order belief of S.

$$\frac{S \mid\equiv CA \Rightarrow Cert_R(t, st), S \mid\equiv CA \mid\equiv Cert_R(t, st)}{S \mid\equiv Cert_R(t, st)} \tag{20}$$

Therefore, S believes in certificate credentials of R, thereby satisfies the goal $G2$. Now, S verifies the signature on message m_2 along with the certificate $Cert_R$. The message m_2 contains an explicit identifier for the intended recipient S. Therefore, S derives that the R said message m_2 and that it was intended for S.

$$\frac{S \mid\equiv \wp\kappa(R, K_R), S \mid\equiv \prod(R, K_R^{-1}), S \triangleleft \sigma(\Re(m_2, S), K_R^{-1})}{S \mid\equiv R \mid\sim m_2} \tag{21}$$

Unlike the first round M_1 in the second round M_2, S receives his sequence number as an identifier to ensure that S is the intended recipient and R is the intended sender for m_2. Now, combining (21) with the first order and second order belief derived in (20) and (18), respectively. Hence, satisfies the goal $G4$.

$$\begin{aligned} M_2 &: S \mid\equiv CA \mid\equiv Cert_R(t, st) \\ &: S \mid\equiv Cert_R(t, st) \text{ and } S \mid\equiv R \mid\sim m_2 \\ &: S \mid\equiv \sigma(\Re(m_2, S), K_R^{-1}) \end{aligned} \tag{22}$$

Hence, satisfy goals $G3$ and $G4$ as derived in the (17) and (22), S believes that R said m_2 and similarly, R believes that S said m_1.

Claim 7.1 *No passive adversary can overhear messages between the intended sender and receiver.*

Proof. In the initial two rounds of communication messages are exchanged over a directed laser beam. Hence, due to the physical constraints and *directed point-to-point* characteristic of the laser beam, a passive adversary may not be able to overhear the messages that were directed to some other recipient. Therefore, it is impossible for an adversary to record the messages from a laser beam (directed to some other vehicle) while still allowing the beam to arrive at the intended receiver. Moreover, the communication over the radio wireless channel is encrypted with the session key that is derived independently at both sides. Hence, the passive overhearing is not possible over the laser authentication channel.

Claim 7.2 *No active proxy adversary can simply forward messages to the intended sender or receiver, in order to impersonate transparently.*

Proof. In the first round goal $G1$ is satisfied as per (15). Therefore, the intended receiver R believes in the correctness of certified coupled static attributes and public key from S. In addition, (16) satisfies the goal $G3$. Hence, intended receiver R believes in the correctness of authentication message m_1 and that it is coupled with the certificate $Cert_S$ from intended sender S. Similarly, for second round (20) fulfills the goal $G2$. Now, intended receiver S believes in the correctness of certificate from intended sender R. In order to confirm that the adversary does not replay the messages between intended S and R, receiver S must qualify the goal $G4$ formalized in (21). S confirms the origin according to the goal $G2$, next, it confirms that S is the actual intended recipient and it finds its own sequence number in the signatures generated at the intended sender R. Therefore, the formalization of goal $G4$ and $G2$ completes the authentication between S and R in two rounds. It is important to mention that the qualification of goal $G2$ and $G4$ is crucial to complete the authentication. The second round completes only if the $G4$ is satisfied that clearly verifies the intended recipient as well as the message confidentiality. Hence, the active proxy adversary cannot misdirect the communication without being detected.

Claim 7.3 *No active adversary can derive the session key without extracting the ephemeral secret key exponents.*

Proof: An active adversary cannot modify or retrieve the contents of the past recorded messages. The associated authentication message m_1 and m_2 ensures the session key integrity and avoids any *Key Compromise Attack.* The authentication message m is comprised of ephemeral secret key eSK along with the long term secret key SK hashed together. Moreover, the session key at R is derived using the ephemeral and long term secret key, i.e., eSK_R and SK_R along with the public key PK_S and $g^{H_1(eSK_S,SK_S)}$. In addition, an independent hashing algorithm H_2 is used to generate the one way exponent known as session key K_R. Therefore, the session key derivation is impossible at an active adversary not holding these ephemeral exponents. Hence, the active adversary cannot modify or retrieve the messages between sender and receiver.

7 Conclusion

This paper presents a vehicle authentication scheme based on secure binding between the static and dynamic attributes of a vehicle. The proposed authentication scheme considered a new attack scenario with multiple identical vehicles. The spontaneous vehicle authentication is accomplished through an auxiliary communication channel in association with the conventional radio channel for message exchange. We utilize the fact that every vehicle occupies a unique combination of dynamic attributes such as location and direction. A focused laser beam is used to verify the vehicle dynamics and to transmit the certified attributes coupled with a public key. Therefore, the laser auxiliary communication channel enables a secure message exchange over radio communication channel. In addition, we illustrate that the proposed approach enhances the security over radio communication channel through an application specific adaptation with the existing authentication protocols.

Acknowledgment

The work of the first author is partially supported by Orange Labs under external research contract number 0050012310-C04021, the Rita Altura Trust Chair in Computer Sciences, Lynne and William Frankel Center for Computer Sciences, and Israel Science Foundation (grant number 428/11). The work of the second author is partially supported by fundings from Polish National Science Center (decision number DEC-2013/09/B/ST6/02251). The work of the last author is partially supported by General Motors.

References

1. Dedicated Short Range Communications (DSRC) available at URL: http://grouper.ieee.org/groups/scc32/Attachments.html.
2. IEEE Std 1609.2-2013 (Revision of IEEE Std 1609.2-2006). *IEEE Standard for Wireless Access in Vehicular Environments Security Services for Applications and Management Messages*, pp 1-289, 2013.

3. A. Kim, V. Kniss, G. Ritter, and S. Sloan. An Approach to Communications Security for a Communications Data Delivery System for V2V/V2I Safety: Technical Description and Identification of Policy and Institutional Issues. U.S. Department of Transportation, Research and Innovative Technology Admisitration (RITA), FHWA-JPO-11-130, Nov. 2011.
4. Kenney, J.B. Dedicated Short-Range Communications (DSRC) Standards in the United States. *Proceedings of the IEEE*, 99(7), pp 1162-1182, 2011.
5. M. Beigl. Point & click - interaction in smart environments. In *Lecture Notes in Computer Science in Handheld and Ubiquitous Computing*, 1707, pp 311-313, 1999.
6. M. Burrows, M. Abadi, and R. Needham. A logic of authentication. *ACM Transactions on Computer Systems*, 8(1), pp 18-36, 1990.
7. R. Canetti and H. Krawczyk. Analysis of key-exchange protocols and their use for building secure channels. In *Lecture Notes in Computer Science in Advances in Cryptology EUROCRYPT*, 2045, pp 453-474, 2001.
8. M. K. Chong and H. Gellersen. Usability classification for spontaneous device association. In *Personal Ubiquitous Comput.*, 16(1), pp 77-89, 2012.
9. W. Diffie and M. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6), pp 644-654, 1976.
10. H. Hartenstein and K. Laberteaux. A tutorial survey on vehicular ad hoc networks. *Communications Magazine, IEEE*, 46(6), pp 164-171, 2008.
11. E. Hossain, G. Chow, V. C. M. Leung, R. D. McLeod, J. Mišić, V. W. S. Wong, and O. Yang. Vehicular telematics over heterogeneous wireless networks: A survey. *Computer Communications*, 33(7), pp 775-793, 2010.
12. T. Kindberg and K. Zhang. Secure spontaneous device association. In *Ubiquitous Computing*, 2862, pp 124-131, 2003.
13. K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage. Experimental security analysis of a modern automobile. In *IEEE Symposium on Security and Privacy (SP)*, pp 447-462, 2010.
14. H. Krawczyk. Sigma: The 'sign-and-mac' approach to authenticated Diffie-Hellman and its use in the ike-protocols. In *Lecture Notes in Computer Science Advances in Cryptology - CRYPTO*, 2729, pp 400-425, 2003.
15. A. Kumar, N. Saxena, G. Tsudik, and E. Uzun. A comparative study of secure device pairing methods. In *Pervasive and Mobile Computing*, 5(6), pp 734-749, 2009.
16. B. LaMacchia, K. Lauter, and A. Mityagin. Stronger security of authenticated key exchange. In *Lecture Notes in Computer Science Provable Security*, 4784, pp 1-16, 2007.
17. J. Lee and J. H. Park. Authenticated key exchange secure under the computational diffie-hellman assumption. *IACR Cryptology ePrint Archive*, 2008.
18. U. M. Maurer and S. Wolf. The relationship between breaking the diffie–hellman protocol and computing discrete logarithms. *SIAM Journal on Computing*, 28(5), pp 1689-1721, 1999.
19. R. Mayrhofer and M. Welch. A human-verifiable authentication protocol using visible laser light. In *The Second International Conference on Availability, Reliability and Security*, pp 1143-1148, 2007.
20. J. McCune, A. Perrig, and M. Reiter. Seeing-is-believing: Using camera phones for human-verifiable authentication. In *IEEE Symposium on Security and Privacy*, pp 110-124, 2005.
21. L. H. Nguyen and A. W. Roscoe. Authentication protocols based on low-bandwidth unspoofable channels: A comparative survey. *Journal of Computer Security*, 19(1), pp 139-201, 2011.
22. P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J.-P. Hubaux. Secure vehicular communication systems: Design and architecture. *Communications Magazine, IEEE*, 46(11), pp 100-109, 2008.
23. S. Patel and G. Abowd. A 2-way laser-assisted selection scheme for handhelds in a physical environment. In *Lecture Notes in Computer Science Ubiquitous Computing*, 2864, pp 200-207, 2003.
24. F. Ponte Mller, L. Navajas, and T. Strang. Characterization of a laser scanner sensor for the use as a reference system in vehicular relative positioning. In *Communication Technologies for Vehicles*, 7865, pp 146-158, 2013.
25. M. Raya and J.-P. Hubaux. The security of vanets. In *Proceedings of the 2nd ACM international workshop on Vehicular ad hoc networks*, pp 93-94, 2005.
26. M. Raya and J.-P. Hubaux. Securing vehicular ad-hoc networks. *Journal of Computer Security*, 15(1), pp 39-68, 2007.
27. M. Ringwald. Spontaneous interaction with everyday devices using a pda. In *Proceedings on Supporting Spontaneous Interaction in Ubiquitous Computing Settings, a workshop held at Ubicomp*, 2002.

28. Tranposrtation Research Board of the National Academies. Guidelines for the Use of Mobile LIDAR in Transportation Applicaions. National Coperative Highway Research Program, Report 748, 2013. http://www.trb.org/Main/Blurbs/169111.aspx
29. A. Sarr, P. Elbaz-Vincent, and J.-C. Bajard. A new security model for authenticated key agreement. In *Security and Cryptography for Networks*, 6280, pp 219-234, 2010.
30. M. Sichitiu and M. Kihl. Inter-vehicle communication systems: A survey. *Communications Surveys Tutorials, IEEE*, 10(2), pp 88-105, 2008.
31. Sufatrio and R. H. C. Yap. Extending ban logic for reasoning with modern pki-based protocols. In *IFIP International Conference on Network and Parallel Computing*, pp 190-197, 2008.
32. L. Ulrich. Whiter brights with lasers. In *IEEE Spectrum*, 50(11), pp36-56, 2013.
33. B. Ustaoglu. Obtaining a secure and efficient key agreement protocol from (h)mqv and naxos. In *Designs, Codes and Cryptography*, 46(3), pp 329-342, 2008.
34. T. Yashiro, T. Kondo, K. Ariyasu, and Y. Matsushita. An inter-vehicle networking method using laser media. In *IEEE 44th Vehicular Technology Conference*, 1, pp 443-447, 1994.
35. B. Fortin, R. Lherbier, and J.C. Noyer. A PHD approach for multiple vehicle tracking based on a polar detection method in laser range data. In *IEEE International Systems Conference (SysCon)*, pp 262-268, 2013.
36. M. Thuy, and F.P. Leon. Non-linear, shape independent object tracking based on 2d lidar data. In *IEEE Intelligent Vehicles Symposium*, pp 532-537, 2009.
37. S. Dolev, Ł. Krzywiecki, N. Panwar, and M. Segal. Vehicle authentication via monolithically certified public key and attributes. In *Wireless Networks*, pp 1-18, 2015.
38. S. Dolev, Ł. Krzywiecki, N. Panwar, and M. Segal. Dynamic Attribute Based Vehicle Authentication. In *Proceedings of the 13th IEEE International Symposium on Network Computing and Applications (NCA)*, pp 1-8, 2014.
39. S. Dolev, Ł. Krzywiecki, N. Panwar, and M. Segal. Optical PUF for Vehicles Non-Forwardable Authentication. Technical report TR-1502, 2015.
40. R.A. MacLachlan, and C. Mertz. Tracking of Moving Objects from a Moving Vehicle Using a Scanning Laser Rangefinder. In *IEEE Intelligent Transportation Systems Conference*, pp 301-306, 2006.
41. O. Abumansoor, and A. Boukerche. Preventing a DoS Threat in Vehicular Ad-hoc Networks using Adaptive Group Beaconing. In *Proceedings of the 8th ACM symposium on QoS and security for wireless and mobile networks*, pp 63-70, 2012.
42. S. Capkun, M. Cagalj, R.K. Rengaswamy, I. Tsigkogiannis, J.P. Hubaux, and M.B. Srivastava. Integrity Codes: Message Integrity Protection and Authentication over Insecure Channels. *IEEE Transactions on Dependable and Secure Computing*, 5(4), pp 208-223, 2008.
43. A. Waytz, J. Heafner, and N. Epley. The mind in the machine: Anthropomorphism increases trust in an autonomous vehicle. *Journal of Experimental Social Psychology*, 52, pp 113-117, 2014.
44. D.A. Thornton and K. Redmill and B. Coifman. Automated parking surveys from a LIDAR equipped vehicle. *Transportation Research Part C: Emerging Technologies*, 39, pp 23-35, 2014.
45. W. Zou, and S. Li. Calibration of Nonoverlapping In-Vehicle Cameras With Laser Pointers. *IEEE Transactions on Intelligent Transportation Systems*, 99, pp 1-12, 2014.
46. Y. Shikiji, K. Watari, K. Tsudaka, T. Wada, and H. Okada. Novel vehicle information acquisition method using vehicle code for automotive infrared laser radar. In *Telecommunication Networks and Applications Conference (ATNAC), Australasian*, pp 52-57, 2014.
47. J. Guillory, S. Meyer, I. Sianud, A.M. Ulmer-moll, B. Charbonnier, A. Pizzinat, and C. Algani. Radio-Over-Fiber Architectures. *IEEE Vehicular Technology Magazine*, 5(3), pp 30-38, 2010.
48. K. David, S. Dixit, and N. Jefferies. 2020 Vision. *IEEE Vehicular Technology Magazine*, 5(3), pp 22-29, 2010.
49. J.A. Larcom, and Hong Liu. Modeling and characterization of GPS spoofing. In *IEEE International Conference on Technologies for Homeland Security*, pp 729-734, 2013.
50. L. Ulrich. Top ten tech cars. *IEEE Spectrum*, 51(4), pp 38-47, Apr. 2014.
51. D. He, N. Kumar, and N. Chilamkurti. A secure temporal-credential-based mutual authentication and key agreement scheme with pseudo identity for wireless sensor networks. *Information Sciences*, 321, pp 263-277, 2015.
52. K. Chain, K.H. Chang, W.C. Kuo, and J.F. Yang. Enhancement authentication protocol using zero-knowledge proofs and chaotic maps. *International Journal of Communication Systems*, 2015.
53. R. Amin, and G.P. Biswas. A secure light weight scheme for user authentication and key agreement in multi-gateway based wireless sensor networks. *Ad Hoc Networks*, 2015.
54. M. Barbeau, J. Hall, and E. Kranakis. Detecting Impersonation Attacks in Future Wireless and Mobile Networks. In *Proceedings of the First international conference on Secure Mobile Ad-hoc Networks and Sensors (MADNES)*, 4074, pp 80-95, 2005.