Dynamic Attribute Based Vehicle Authentication

(Extended Abstract)

Shlomi Dolev*, Łukasz Krzywiecki†, Nisha Panwar*, Michael segal‡
*Department of Computer Science
Ben-Gurion University of the Negev, Israel.
{dolev,panwar}@cs.bgu.ac.il
†Institute of Mathematics and Computer Science
Wroclaw University of Technology, Poland.
lukasz.krzywiecki@pwr.wroc.pl
‡Department of Communication Systems Engineering
Ben-Gurion University of the Negev, Israel.
segal@cse.bgu.ac.il

Abstract*—In the near future, vehicles will establish a spontaneous connection over a wireless radio channel, coordinating actions and information. Security infrastructure is most important in such a hazardous scope of vehicles communication for coordinating actions and avoiding accidents on the roads. One of the first security issues that need to be established is authentication. Vehicle authentication with visual binding prior to establishing a wireless radio channel of communication is useful only when the vehicles possess unique visual attributes. These vehicle static attributes (e.g., licence number, brand and color) are certified together with the vehicle public key. Therefore, we consider the case of 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 vehicles. 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 NAXOS, in the new scope of ad-hoc vehicle networks.

Keywords*—*Certificate authority, security, vehicular networks.

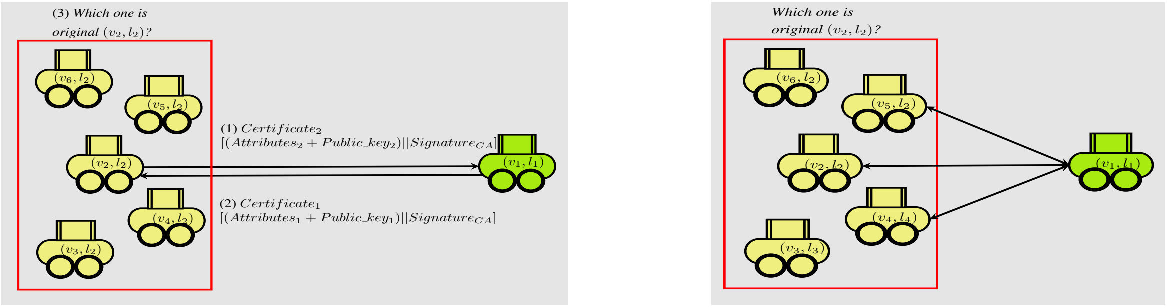
I. Introduction

Communication security in the scope of vehicle networks [7], [8], [26] introduces new sensitive challenges. A voluntary association among vehicles require a robust authentication mechanism. For example, an instant warning message from a vehicle in front requires an instant authentication before the receiving vehicle reacts according to that warning message. It might worsen into a life threatening situation if the adversary is able to fake these warning messages.

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 same peer vehicle visualized over the auxiliary channel. However, the constantly moving vehicles may not be identified solely on the basis of visual attributes. Therefore, we couple non-certified dynamic attribute (e.g., location and direction) of any vehicle along with the certified coupled list of static attributes and the public key of a 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 in a way that can be verified accurately. Since dynamic attributes cannot be certified beforehand, we propose to utilize a directional laser beam to bind the dynamic attributes with the certified coupled static attributes and the public key. We illustrate a scenario with multiple maliciously identical vehicles, whereas a communicating vehicle is not able to distinguish the authentic vehicle through the certified static attributes only. Every vehicle needs to generate and dispatch the messages from its own laser interface. Therefore, the sender is accountable for any fake messages sent and received by its own interface. Moreover, the corresponding receiver can also claim at the sender and then the sender is held responsible and can be penalized for sending fake messages.

According to our previous work [33], 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 scenario.

Problem statement. We consider a scenario in which vehicles are allowed to communicate over the IEEE 802.11p wireless radio channel. However, the inherently vulnerability of radio communication might impose severe impersonation attacks leading to a strategic crash. 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 vehicle 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 for any vehicle. First, there must be a binding between the certified


(3) *Which one is original* (v_2, l_2)?
(v_6, l_2)
(v_5, l_2)
(v_2, l_2)
(v_4, l_2)
(v_3, l_2)
(v_1, l_1)
(1) $Certificate_2$ $[(Attributes_2 + Public\_key_2)||Signature_{CA}]$
(2) $Certificate_1$ $[(Attributes_1 + Public\_key_1)||Signature_{CA}]$
Which one is original (v_2, l_2)?
(v_6, l_2)
(v_5, l_2)
(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. 1: Multiple maliciously identical vehicles.

static attributes and the non-certified dynamic attributes of the vehicle. Second, there must be a binding between two communication channels, i.e., a directed laser beam to convey the certified attributes and a secure wireless radio channel to convey the session messages.

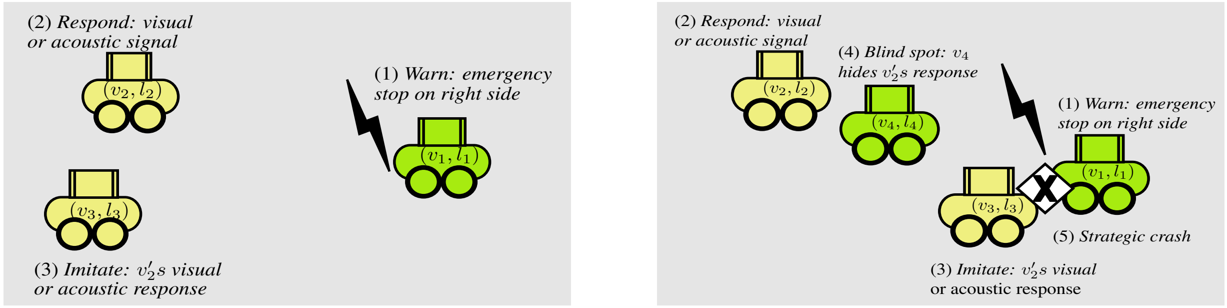
Previous work. In this section, we illustrate the related work, concerning spontaneous wireless vehicle network security threats [10] such as message tempering [36], impersonation [37] and denial of service attack (DoS) [35]. It is important to mention that vehicles utilize wireless communication standard, i.e., IEEE 802.11p Wireless Access in Vehicular Environment (WAVE) based IEEE 1609 Dedicated Short Range Communication (DSRC) [1].Raya and Haubaux [19], [22], [23] 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. Our scheme removes the active participation of roadside units as well as the regional authorities.

The state-of-the-art for the wireless and out-of-band channel association can be found in [12]. It is important to mention that the vehicles tracking through the laser beam pointing and scanning is feasible in practice [31], [32], [34] and can be installed and used by a moving vehicle. Laser communication in vehicular networks has been primarily used for distance and velocity estimation [21], [30]. In [2], [24], laser pointers are used for spontaneous ping among the hand held devices. The work in [20] presents a laser modulation technique to transmit the device network address. 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 [9], the authors suggest the transmission of the shared secret key through the laser modulation. It has the same drawback as with the previous approach [20] that is an adversary equipped with a high resolution camera might capture the laser beam modulation to recover the secret session key. Another work, in [17], 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. In [16], the authors presented a scheme with commitment verification on a laser channel while using Diffie-Hellman [6] key exchange on a wireless radio channel beforehand. The drawback with this approach is that 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 [18] presents a classification of one-way, two-way and group authentication protocols based on the *commitment before knowledge* principle. The authors in [5] present 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.

Our contribution.

- We extend the authentication mechanism within the scope of non-certified dynamic attributes of any vehicle. The proposed approach provides a secure binding between two communication channels, i.e., auxiliary and radio communication channel for the authentication and warning message exchange, respectively.
- 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, such as laser or directed antenna, used to change and verify periodically processed and digitally signed certificates.

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. 6). 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 for channel contention among the communicating vehicles 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


(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)
X
(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. 2: Strategic crash by maliciously identical vehicles.

authentication overhead for the usage of shared communication band. We prove the security of our scheme using BAN Logic [3], [27] the proof is omitted from this extended abstract due to space restriction.

Outline. Section II describes a crash scenario and we provide a solution to avoid such a scenario through secure visual binding with respect to auxiliary as well as radio communication channel. A detailed description of the proposed approach is given in Section III. Section IV 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 V. Section VI overviews a coalition attack scenario and the direction for solution in near future. Furthermore, Section VII concludes the discussion on the security of the proposed approach.

II. Attack Scenarios on Static Attribute based Scheme

The *static attribute verification* seems imperfect in a scenario where the adversary encompasses multiple identical vehicles that indeed impersonate a target vehicle, see Fig. 1 and Fig. 2. Vehicles are moving from left to right in all the figures.

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. 1. 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. 1. 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. However, 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. 2, 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 using the secured wireless communication, 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.

The other way, 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.

World Manufacturer Identifier (geographic area, country, plant code)	
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)	
Vehicle Indicator Section (engine number, engine type, license number, chassis number)	
GPS Device Identification	Wireless Device Fingerprint
Procedures to Execute for Verifying the Attributes	
Certificate Sequence Number	Certificate Expiration Date
Public Key	
Digital Signature	

Fig. 3: Certificate structure

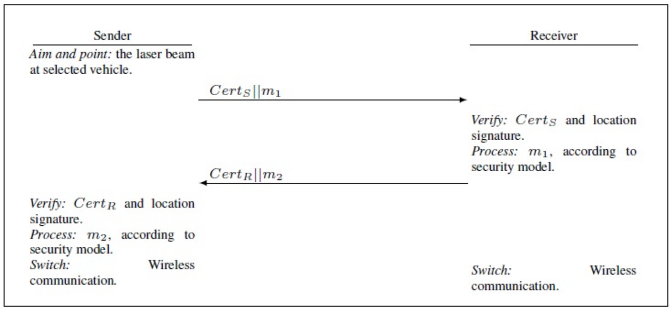

Sender
Receiver
Aim and point: the laser beam at selected vehicle.
$Cert_S||m_1$
Verify: $Cert_S$ and location signature.
Process: m_1, according to security model.
$Cert_R||m_2$
Verify: $Cert_R$ and location signature.
Process: m_2, according to security model.
Switch: Wireless communication.
Switch: Wireless communication.

Fig. 4: The proposed approach.

III. Dynamic and Static Attributes based Scheme

We aim to verify dynamic attributes along with the 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. 3) is used that conveys the certified coupled public key and static attributes, i.e., $Cert$ $= Attribute{+}PK||Sign_{CA}(Attribute{+}PK)$. Subsequently, third round of message exchange over the wireless radio channel is considered implicit. We next list our assumptions.

Assumptions and mathematical background.

- Vehicles communicate in the presence of *Public Key Infrastructure* that provides periodic certification service.
- Only CA can certify the static attributes and public key using a secret key, however, vehicles 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.
- Laser beam pointed at the target vehicle cannot be interrupted by the attacker without prohibiting the beam to arrive at the target vehicle.
- Vehicles are assumed to be active on a wireless radio channel in order to exchange safety critical warning messages. However, auxiliary communication through a laser beam is utilized for a point-to-point targeted communication where sender vehicle selects and points laser beam at target vehicle. Therefore, sender vehicle utilizes a laser channel in order to create a secure binding between the laser and radio communication channel with respect to a particular target vehicle.

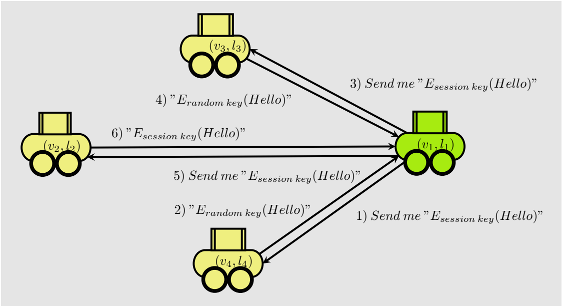
As the presented key agreement protocol and the associated authentication protocols are based on Diffie-Hellman (DH) key exchange, so we assume that corresponding computations are done within a group $G = \langle g \rangle$ of prime order q, where Computational Diffie-Hellman (CDH) assumption holds.

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 [15] within the cyclic group G.

Proposed approach. In Fig. 4, 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 vehicle selects a vehicle for communication and points the laser beam. 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 sender, i.e., m_1 is received and processed as per the associated security model. 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, receiver forwards its own certificate $Cert_R$ accompanied with the authentication message m_2 over laser channel. Sender verifies the attribute binding with the public key and processes the message m_2 as per the associated security model. Readers may refer to a detailed description about the proposed scheme in the Section IV.

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, for example, the location attributes. All notations used for the proposed approach are given in Table I.


(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. 5: Re-authentication.

In our scheme v_S can identify v_R among the group of maliciously identical vehicles (similar as v_2), see Fig. 5. 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

Table I: Notations.

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
$Attributes_S$	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 for certificate verification	K	Session key with NAXOS adaptation
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

requests for a session key 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.

IV. Binding with the Existing Protocol

Our approach provides a straight binding between the vehicle location, 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 [11], NAXOS [13], NAXOS+ [14], CMQV [29], SMQV [25] already proven to be secure in existing models such as CK [4], eCK [13] and seCK [25]. 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, without the loss of generality 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.
  - 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 additional two rounds to establish a secret session key among the parties. Apparently, this is not the case in our protocol, here it requires overall 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. 6. 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.

V. Security Discussion

In this section, we discuss the protocol security against the passive and active adversary.

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.

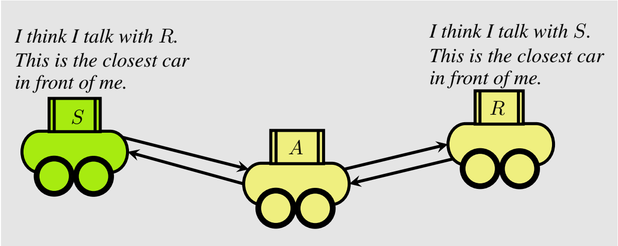
Active adversary. An active impersonation, see Fig. 7, allows the adversary to *intercept, remove, skip, delay, manipulate* or *insert fake* messages, in a *man-in-the-middle* manner. Here, we assume that the adversary is equipped with the double laser interfaces (e.g. in front, and at the back of the 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

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. 6: Adapted NAXOS protocol.

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 exactly *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 exactly 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, see Fig. 8 on the left side.



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

Fig. 7: Misbinding scenario.

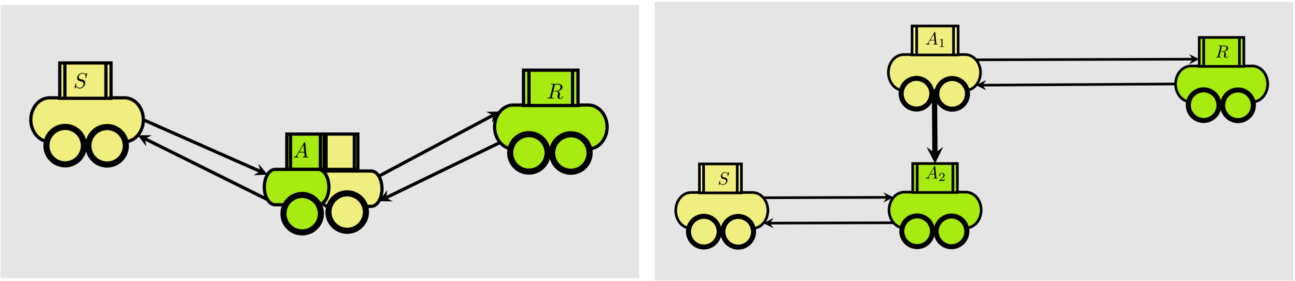
- The active adversary tries to *manipulate* or *insert fake* messages. The intended sender and receiver exchange the messages with a false impression that they communicate directly to each other. Whereas, the active adversary with exactly *matching static attributes* sits in the middle and either modifies or injects fake message to each other, correspondingly. However, the binding between augmented certificate and laser communication channel does not weaken the security of the associated authentication protocol, such as NAXOS, which is already proven to be secure in the assumed model. Furthermore, our approach guarantees to resolve the vehicle identity in the presence of multiple identical vehicles.

VI. Coalition of Adversaries

We are not considering the coalition attack scenario in this paper, see Fig. 8. According to the coalition scenario, there exists two or more malicious vehicles between the sender and the receiver. One of these malicious vehicles impersonates sender and the other impersonates receiver by carrying exactly similar static attributes. Moreover, these malicious vehicles communicate over a separate communication channel to relay the messages between actual sender and receiver. Although malicious vehicles may not be able to decipher the messages, however, malicious vehicles can create an illusion of correct visual binding. The sender believes that it forwards message to receiver while actually forwarding it to one of the malicious vehicle impersonating the receiver and vice versa. It must be noticed that coalition scenario cannot be avoided with the proposed configurations and additional assumptions are required. In order to mitigate this coalition attack scenario and to identify the recipient vehicle (while keeping the directed nature of the channel), we plan to utilize an *enhanced wireless fingerprinting* approach in near future.

VII. Conclusion

The paper presents a vehicle authentication scheme based on secure binding between the static *and* dynamic attributes of a vehicle. 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, distance, velocity 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



On the left side scenario, adversary A in the middle has some visible attributes of both S and R at the same time which is relatively unlikely. However, scenario on right side illustrates the coalition of adversaries that requires additional assumptions to avoid such a scenario. Accordingly, A_1 impersonates S and A_2 impersonates R by assuming similar visible static attributes. Henceforth, adversaries communicate over some additional channel and relay the messages between S and R, without deciphering those messages. As a result of which S misinterprets A_2 as R and R misinterprets A_1 as S.

Fig. 8: Coalition of adversaries.

auxiliary communication channel enables a secure message exchange over radio communication channel. The proposed authentication scheme consider to avoid a new attack scenario with multiple identical vehicles. In addition, we illustrate that the proposed approach enhances the security over radio communication channel through the binding with the existing and proven 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] M. Beigl. Point & click - interaction in smart environments. In *Handheld and Ubiquitous Computing*, 1999.

[3] M. Burrows, M. Abadi, and R. Needham. A logic of authentication. *ACM Trans. Comput. Syst.*, 1990.

[4] R. Canetti and H. Krawczyk. Analysis of key-exchange protocols and their use for building secure channels. In *Advances in Cryptology EUROCRYPT 2001*.

[5] M. K. Chong and H. Gellersen. Usability classification for spontaneous device association. *Personal Ubiquitous Comput.*, 2012.

[6] W. Diffie and M. Hellman. New directions in cryptography. *Information Theory, IEEE Transactions on*, 1976.

[7] H. Hartenstein and K. Laberteaux. A tutorial survey on vehicular ad hoc networks. *Communications Magazine, IEEE*, 2008.

[8] 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. *Comput. Commun.*, 2010.

[9] T. Kindberg and K. Zhang. Secure spontaneous device association. In *Ubiquitous Computing*. 2003.

[10] 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 *In IEEE Symposium on Security and Privacy (SP)*, 2010.

[11] H. Krawczyk. Sigma: The 'sign-and-mac' approach to authenticated Diffie-Hellman and its use in the ike-protocols. In *CRYPTO*, 2003.

[12] A. Kumar, N. Saxena, G. Tsudik, and E. Uzun. A comparative study of secure device pairing methods. *Pervasive and Mobile Computing*, 2009.

[13] B. LaMacchia, K. Lauter, and A. Mityagin. Stronger security of authenticated key exchange. In *Provable Security*. 2007.

[14] J. Lee and J. H. Park. Authenticated key exchange secure under the computational diffie-hellman assumption. *IACR Cryptology ePrint Archive*, 2008.

[15] U. M. Maurer and S. Wolf. The relationship between breaking the diffie–hellman protocol and computing discrete logarithms. *SIAM J. Comput.*, 1999.

[16] R. Mayrhofer and M. Welch. A human-verifiable authentication protocol using visible laser light. In *Availability, Reliability and Security*, 2007.

[17] J. McCune, A. Perrig, and M. Reiter. Seeing-is-believing: Using camera phones for human-verifiable authentication. In *Security and Privacy, 2005 IEEE Symposium on*.

[18] L. H. Nguyen and A. W. Roscoe. Authentication protocols based on low-bandwidth unspoofable channels: A comparative survey. *J. Comput. Secur.*, 2011.

[19] 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*, 2008.

[20] S. Patel and G. Abowd. A 2-way laser-assisted selection scheme for handhelds in a physical environment. In *Ubiquitous Computing*, Lecture Notes in Computer Science. 2003.

[21] 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*. 2013.

[22] M. Raya and J.-P. Hubaux. The security of vanets. In *Proceedings of the 2nd ACM international workshop on Vehicular ad hoc networks*, 2005.

[23] M. Raya and J.-P. Hubaux. Securing vehicular ad-hoc networks. *Journal of Computer Security*, 2007.

[24] M. Ringwald. Spontaneous interaction with everyday devices using a pda, 2002. In *Proc. Supporting Spontaneous Interaction in Ubiquitous Computing Settings, a workshop held at Ubicomp*, 2002. http://www.dcs.gla.ac.uk/ pd/Workshops/papers/ringwald.pdf.

[25] A. Sarr, P. Elbaz-Vincent, and J.-C. Bajard. A new security model for authenticated key agreement. In *Security and Cryptography for Networks*. 2010.

[26] M. Sichitiu and M. Kihl. Inter-vehicle communication systems: A survey. *Communications Surveys Tutorials, IEEE*, 2008.

[27] 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, 2008*.

[28] L. Ulrich. Whiter brights with lasers. In *IEEE Spectrum*, 2013.

[29] B. Ustaoglu. Obtaining a secure and efficient key agreement protocol from (h)mqv and naxos. *Designs, Codes and Cryptography*, 2008.

[30] T. Yashiro, T. Kondo, K. Ariyasu, and Y. Matsushita. An inter-vehicle

networking method using laser media. In *Vehicular Technology Conference, IEEE 44th*, 1994.

[31] Fortin, B. and Lherbier, R. and Noyer, J.C. A PHD approach for multiple vehicle tracking based on a polar detection method in laser range data. In *Systems Conference (SysCon), IEEE International*, 2013.

[32] Thuy, M. and Leon, F.P. Non-linear, shape independent object tracking based on 2d lidar data. In *Intelligent Vehicles Symposium, IEEE*, 2009.

[33] S. Dolev, L. Krzywiecki, N. Panwar, and M. Segal. Certificating Vehicle Public Key with Vehicle Attributes. In *ASCoMS (Architecting Safety in Collaborative Mobile Systems) at SAFECOMP*, 2013.

[34] MacLachlan, R.A. and Mertz, C. Tracking of Moving Objects from a Moving Vehicle Using a Scanning Laser Rangefinder. *Intelligent Transportation Systems Conference, IEEE*, 2006.

[35] O. Abumansoor, and A. Boukerche. Preventing a DoS Threat in Vehicular Ad-hoc Networks using Adaptive Group Beaconing. *Proceedings of the 8th ACM symposium on QoS and security for wireless and mobile networks*, 2012.

[36] 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 Trans. Dependable Sec. Comput.*, 2008.

[37] M. Barbeau, J. Hall, and E. Kranakis. Detecting Impersonation Attacks in Future Wireless and Mobile Networks. Proceedings of the First international conference on Secure Mobile Ad-hoc Networks and Sensors (MADNES), 2005.