Certificating Vehicle Public Key with Vehicle Attributes A (periodical) Licensing Routine, Against Man-in-the-Middle Attacks and Beyond

Shlomi Dolev, Łukasz Krzywiecki, Nisha Panwar, Michael Segal

Certificating Vehicle Public Key with Vehicle Attributes

A (periodical) Licensing Routine, Against Man-in-the-Middle Attacks and Beyond

(Extended Abstract)

Shlomi Dolev[1] Łukasz Krzywiecki[2] Nisha Panwar[1] Michael Segal[3]

[1] Department of Computer Science, Ben-Gurion University of the Negev, Israel.
{dolev, panwar}@cs.bgu.ac.il. *
[2] Institute of Mathematics and Computer Science, Wroclaw University of Technology, Poland.
lukasz.krzywiecki@pwr.wroc.pl.
[3] Department of Communication Systems Engineering, Ben-Gurion University of the Negev, Israel.
segal@cse.bgu.ac.il. **

Abstract. Vehicular networks are used to coordinate actions among vehicles in traffic by the use of wireless transceivers. Unfortunately, the wireless communication among vehicles is vulnerable to security threats that may lead to very serious safety hazards. In this work we propose a viable solution for coping with Man-in-the-Middle attacks. To the best of our knowledge, this is the first work that propose to certify both the public key and out-of-band sense-able attributes to enable mutual authentication of the communicating vehicles. Vehicle owners are bound to preprocess (periodically) a certificate for both a public key and a list of fixed unchangeable attributes of the vehicle.

Keywords: Man-in-the-Middle attack, security, vehicular network.

1 Introduction

Security is a major concern in vehicular network where on one hand the wireless, ad-hoc and mobile communication imply security threats, and on the other hand requires perfectly reliable communication, as errors have immediate hazardous implications [56]. While vehicles move in a predictable road topology, maneuvering among the vehicles is somewhat unpredictable. For example, the vehicle ordering is changed dynamically along the road.

Applications for vehicular networks: Gaining on road safety and efficient traffic management are two prime goals in the use of vehicular networks. Smart vehicles may exchange information concerning road scenario with each other to help manage the traffic and to address safety concerns [25]. For example, a notification on the occurrence

* Partially supported by Rita Altura Trust Chair in Computer Sciences, Lynne and William Frankel Center for Computer Sciences, Israel Science Foundation (grant number 428/11).
** The work of Michael Segal has been supported by General Motors Corporation.

of an accident or a traffic jam ahead may assist the approaching vehicles to optimize their time and energy resources. In the very near future, vehicle will interact with several other vehicles on a daily trip to coordinate actions [29].

Recently, several major projects [1] such as Car2Car-Communication Consortium [2], Cartalk [3], Network on Wheels [4], Vehicle Infrastructure Integration [5], Partners for Advanced Transportation Technology [6], Secure Vehicular Communication [7], E-safety Vehicle Intrusion protected Applications [8] were conducted in order to initiate, develop and standardize the vehicle networks operation. These projects were funded by national governments and accomplished by a joint venture of automobile companies, universities and research organizations.

Customized standard and hardware for vehicles: Modern vehicles are equipped with Electronic Control Units (ECU), sensors, actuators [31] and wireless transceiver that supports the DSRC (Dedicated Short Range Communication) standard [19, 9] thus, enabling the creation of vehicle networks. ECU's are interlinked to trigger a collaborative decision on some safety critical event. Vehicles are equipped with local in-vehicle network and a wireless gateway to interface the in-vehicle network with the outside communication devices. In-vehicle network can be divided into controller area network (CAN), local interconnect network (LIN), and media oriented system (MOST) [35]. These embedded devices enable facilities such as automatic door locking, collision warning, automatic brake system, reporting road condition, rain and dark detection and communication with the surrounding road infrastructure.

Registration and identity certification: Currently, every vehicle is periodically registered with its national or regional transportation authority, which allocates a unique identifier to the vehicle with an expiration date which is the next required inspection date. In some regions of the US and the EU, registration authorities have made substantial progress toward electronically identifying vehicles and machine readable driving license. Moreover, these registration authorities assign a private/public key pair to the inspected vehicles.

Man-in-the-Middle (MitM) attack in vehicle networks: Identifying a vehicle is crucially important in the scope of establishing secure communication with passing by vehicles. In particular, when using public key infrastructure to establish a private key among vehicle pairs in order to communicate on the road. One disadvantage of the public key infrastructure is the need to cope with MitM attacks. The following scenario demonstrates a typical MitM attack.

The scenario starts when a vehicle v_1 tries to securely communicate with v_2, requesting for the public key. Vehicle v_3 pretends to be v_2 and answers v_1 with v_3 public key instead of v_2. Then v_3 concurrently asks v_2 for its public key. Vehicle v_1 is fooled to establish a private key with v_3 instead of v_2, and v_2 is fooled to establish a private key with v_3 instead of v_1. Vehicle v_3 conveys messages from v_1 to v_2 and back decrypting and re-encrypting with the appropriate established keys. In this way v_3 can find the appropriate moment to change information and cause hazardous actions to v_1 and v_2.

For example, consider three vehicles v_1, v_2 and v_3 with different brands and license numbers. Vehicle v_1 wants to establish a key with v_2, a Mercedes-Benz with license number l_2, and send a request for a public key, specifying that it would like to set a

secret session key with the Mercedes-Benz that carries the license number l_2. At this point v_3 which is a Toyota with license number l_3 intercepts and sends its public key as if it belongs to the Mercedes-Benz that carries the license number l_2. Now, v_1 can verify that the received public key (of v_3 pretending to be v_2) has been legally produced by the CA, and may fooled to establish a secret session key with v_3. Thus, v_1 confirms the public key authenticity but cannot be sure whether it just verified a Mercedes-Benz with license number l_2 or a Toyota that pretends to be a Mercedes-Benz with license number l_2. To avoid such a design that is sensitive to MitM attacks we suggest to certify both the public key and the attribute together in a monolithic fashion. This is possible by having the certified linked fixed attributes together with the public key.

Public key infrastructure has a severe disadvantage when coping with MitM attacks not only in the scope of vehicle networks. Even when the certificate authority (CA) signs the public key, the public key owner should be identified by out-of-band means to cope with signed certificate thefts [47]. We propose a solution that employs vehicles fixed attribute based certification mechanism to correctly identify the neighboring vehicles. The periodic licensing routine can serve as an important ingredient of our scheme. Our method has the benefit of interacting with the CA only during preprocessing stages, rather than during the real-time secret session key establishment procedure. The certified attributes may be visually verified by a camera, microphone, wireless transceiver fingerprint identification [23], and/or other sensing devices which will feed the received data to, say, machine learning based classifier that will approve that indeed the attributes in the certificate match the sensed attributes of the vehicle. Visual identification may imply a better authentication of the transmission source in comparison with noise and/or transceiver fingerprint. Therefore, the trust level in the information communicated by a neighbor, and the type of actions taken according to the information received from the neighbor, may depend on the current set of attributes verified by out-of-band means.

Our solution relies on the CA approval that the public key was originated by the CA, and that the public key belongs to the vehicle with the coupled signed attributes. Given such certified public key and vehicle attributes, we are able to establish a secret session key with neighboring authenticated vehicle using only two communication rounds. Once the session key is established vehicles can securely exchange messages.

The paper is organized into four sections. Next, subsection highlights the related work regarding security threats, mitigating man-in-the-middle attacks, entity authentication and out-of-band channel authentication. In Section 2 a detailed description of the proposed work has been given. In Section 3 we discuss properties of our proposition in relation to security provided by other key establishment protocols. Section 4 highlights the transport layer security handshake with certified attributes. The last Section 5 concludes the discussion on the proposed scheme. Proofs are omitted from this extended abstract.

Related Work. In what follows, we describe in more details the related work, concerning vehicle networks threats, the state of art for mitigating MitM attacks. Then we describe existing entity authentication schemes, and in particular, the use of group coordination and distance maintenance.

Vehicle networks threats: Autonomous wireless connection among vehicles imposes serious security threats such as eavesdropping [54], identity spoofing [21, 53], sybil attack [42], wormhole attack [46], replay attack [62], message content tempering [20], impersonation [16], denial of service attack (DoS) [15] and man-in-the-middle attack [33].
Mitigating Man-in-the-Middle attacks: Global System for Mobile Communication (GSM) is one of the most popular standards. Unfortunately, it uses only one sided authentication between the mobile station and the coupled base station [10]. Universal Mobile Telecommunication Standard (UMTS) improves over the security loopholes in GSM. It includes a mutual authentication and integrity protection mechanism but is still vulnerable to MitM attacks [60].

MitM and DoS attack analysis for Session Initiation Protocol (SIP) is shown in [22], using a triangle communication model between SIP user agent and server. This work presents an analysis on the attack possibility, but does not offer any solution to the problem in hand. The interconnection between 3G and wireless LAN is vulnerable to MitM attacks by influencing the gateway nodes [63]. According to [34] mobile host and base station shares a secret cryptographic functions and mutually raises a challenge-response string, prior to employing the original Diffie-Hellman key exchange scheme [24]. Thus, mobile host replies with a cryptographic response and Subscriber Station Identifier (SSI) to base station, but it does not verify any of the unchangeable attributes of the intended subscriber. This way a base station, capable of verifying a unique SSI connection, may not confirm the authentic owner of the SSI connection.
Entity authentication: There has been a great research activity in the scope of cryptographic solutions [48] for entity authentication. A security scheme for sensor networks, called TESLA has been proposed in [49]. TESLA is based on delayed authentication with self-authenticating key chains. TESLA yields a time consuming authentication mechanism (as the messages received on a timeline, can be authenticated, only after receiving the immediate next message over the same timeline). Although, chances are less but still a man-in-the-middle can intercept through weak hash collisions and fake delayed key. An improvement TESLA++ has been suggested in [59], as an adapted variation of delayed authentication. A combination of TESLA++ and digital signature provides Denial of Service (DoS) attack resilience and non-repudiation respectively. The drawback with this approach is that message digest and corresponding message (with self-authenticating key) is transmitted separately to the receiver. Thus, man-in-the-middle may step in, as it does not follow the fixed attribute based verification.

Raya and Haubaux [51, 52] proposed that each vehicle contains a set of anonymous public/private key pairs, while these public keys have been certified by CA. The certificates are short lived and therefore needs to be confirmed with a Certificate Revocation List (CRL) before the use. The drawback with this approach is that road-side infrastructure is required to provide the most updated CRL. A man-in-the-middle attack resistant key agreement technique for peer to peer wireless networks appears in [18] where primary mutual authentication is done before the original Diffie-Hellman key exchange. This primary authentication step could be secret digest comparison, e.g., through visual or verbal contact, distance bounding or integrity codes. A

man-in-the-middle can intercept because the proximity awareness, visual and verbal signals are computed by the device and verified by the user; while in our case it is already certified by CA and then user verifies it again. The secure communication scheme in [61] is enhancement over the Raya and Haubaux scheme, in that certified public key is exchanged and further used to setup a secret session key as well as group key. Here, the attacker can pretend to be some other vehicle, by replaying the certificates and there exists no other means to verify that this vehicle is not the actual owner of the certificate.

There exists a few one round protocols that ensures weak forward secrecy [13] providing *Forward Secrecy* only when the adversary is not active in the session. These works also proves impossibility for establishing strong forward security when using only one round. One round protocols are based on a simultaneous interaction between the sender and receiver. However, one way protocol with strong secrecy exists in [32, 14, 17]. They have assumed that the ephemeral secret keys are exchanged between the peer parties while the adversary is not allowed to extract any of these ephemeral secret keys.

Our work is the first that demonstrates the utility of out of band identification using coupled public key and fixed verifiable attributes. We ensure the countermeasures against the man-in-the-middle attack in two (sequential) rounds of communication.

Out-of-band channel authentication: There have been great efforts to utilize various auxiliary out-of-band channels for entity authentication. The notion of pre shared secret over a limited contact channel has been raised in [58]. A method shown in [30, 44] suggests that a common movement pattern can help mutually authenticate two individual wireless devices driven by single user. In [57] a pre-authentication phase is required before the original public key is exchanged and confirmed over the insecure wireless channel. Pre-authentication channel is a limited scope channel to share limited information, still it inherits the same vulnerability as wireless channel have. In this scheme there may be cases when a vehicle is not sure that it received data from whom it should receive. In our scheme we do it in reverse first wireless channel authentication and then verification over out-of-band channel, and that too certified by CA during preprocessing.

Another work in [45] presents a visual out-of-band channel. A device can display a two dimensional barcode that encodes commitment data, hence, a camera equipped device can receive and confirm this commitment data with the public key. Unfortunately the attacker can still capture and/or fabricate the visible commitment data, as it is not certified with the public key. The approach in [26] is based on acoustic signals, using audio-visual and audio-audio channels to verify the commitment data. In the former a digest of the public key is exchanged by vocalizing the sentence and comparing with a display on the other device, while the later compares vocalized sentences on both devices. In a recent work [55], Light Emitting Diode (LED) blinks and the time gap between those blinks has been used to convey the digest on the public key. Also, a combination of audio-visual out-of-band channel has been proposed in [50], that uses beeps and LED blinks in a combination to convey the commitment data. The proposed method is less effective because the public key and the out-of-band information are not certified and therefore man-in-the-middle can learn the out-of-band information

and replay it. The approach in [43] suggests the use of spatial reference authentication, which is dynamic and can be manipulated by the man-in-the-middle. Also, the visual laser authentication can be ambiguous due to the equipment and the foggy weather condition unlike our scheme that relies on static sense-able attributes coupled with the public key.

2 Out-of-band Sense-able Certified Attributes for Mitigating Man-in-the Middle Attacks

We suggest mitigating man-in-the-middle attacks by coupling out-of-(the wireless)-band verifiable attributes. Vehicles are authenticated using digitally signed certificates and out-of-band verifiable attributes. For example, these attributes may include visual information that can be verified by input from a camera when there exists line-of-sight, including the identification of the driving license number, brand, color and texture, and even the driver faces if the owner wants to restrict the drivers that may drive the vehicle. Other attributes may be verified by other sensing devices, such as microphone for noise.

Our approach does not require any communication with the certificate authority or the road side units, while actually authenticating vehicles on the move. The only interaction with the CA is during a preprocessing stage, which is mandatory to possess a certificate. The certificate holds a public-key and unchangeable (or rarely changeable) attributes of the vehicle signed by the CA. These out-of-band sense-able vehicular attributes should be sensed by other vehicles and checked in real-time. Note that the procedure to check these vehicular attributes may be given as part of the certified information. Our scheme is a viable solution to combat the man-in-the-middle attacks, as it utilizes a separate sense-able out-of-band channel to authenticate the unchanged vehicular attributes. The certificate can be updated and restored on each periodical inspection or in the rare case of attribute change. Thus, saving time and communication overhead in the authentication process, as well as avoiding a CA communication bottleneck, obtaining a scheme suitable for emergency and safety critical applications. Detailed description of the solution appears in the next section.

In the proposed scheme vehicles carry digitally signed certificate $Cert$ from CA, see Figure 1 for a possible structure of such a certificate. The pseudo-code description of the secret key establishment procedure appears in Figure 2. In the procedure we use PK to denote the public key, SK to denote the private key, key_r is the obtained shared secret session key, H is the shared hashing algorithm and $||$ denotes the appended string value. Note that the $+$ sign denotes a predetermined symmetric composition and accordingly continuous zero bits are padded between the two cipher components. Hence, the cipher components linked with $+$ are verified against the cipher component value as well as the symmetric zero composition between these components.

We assume that the CA established a certificate in the form of $Attribute_S + Publickey_S || E_{SK_{CA}}(H(Attribute_S + Publickey_S))$ for each party. These certificates are used to establish a (randomly chosen) shared key, key_r. The shared key key_r can then be used to communicate encrypted information from the sender to the receiver and back. One way to do this is to use key_r as a seed for producing the same pseudo-random

sequence by both the sender and the receiver. Then XOR-ing the actual sensitive information to be communicated with the bits of the obtained pseudo-random sequence. Next, we describe in detail the involved entities, and their part in the procedure for establishing a session key.

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

Figure 1: Certificate structure

Certificate Authority: The list of CAs with their public keys PK_{CA} may be supplied as an integral part of the transceiver system of the vehicle, similar to the way browsers are equipped with a list of CAs public keys. Only registered vehicles are allowed to communicate on the road. Digital signatures $E_{SK_{CA}}(H(Attribute_{sender} + Public\,key_{sender}))$ represent the hash of public key and attributes encrypted with the CA secret key SK_{CA}. The digital certificate works as an approval over the public key and the out-of-band verifiable attributes of the vehicle. The CA can update or renew a certificate, upon a need, or when the current certificate expires.

Vehicular Attributes: Vehicles incorporate various sensors to capture useful primitive from the neighborhood. Each vehicle is bound to a set of primitives yielding a unique identity to that vehicle. Vehicles identity encloses a tuple comprised of attributes such as license number, public key, distinct visual attributes and other out-of-band sense-able attributes, extending the basic set of attributes required according to ISO 3779 and 3780 standard [11]. These out-of-band sense-able attributes are captured through customized device connections such as camera, microphone, cellular communication and satellite (GPS system). In addition, we suggest to identify the wireless communication itself, rather than the contents sent by the wireless communication, this is done by the certified transceiver fingerprints. Thus, the transceiver must be removed from the original vehicle and possibly be reinstalled in attackers vehicle to launch the attack. Verifying each of the attributes by out-of-band channel implies certain trust level in the identity of the communicating party, which in turn implies the possible actions taken based on the received information from the partially or fully authenticated communicating party. Thus, a vehicle can perceive the surroundings from driver's perspective using vision with a sense of texture, acoustic signals, and the digital certificate. A combination of

these primitives is different for every vehicle, the unique license number observed by the camera, the outlook of the vehicle including specific equipment, or specific visual marks such as specific color repair marks, unique license number, outlook of the vehicle, manufacturer's logo, engine acoustics classification signals. During the communication vehicles continuously exchange the geographic coordinates that can be certified as being received from the certified GPS device, according to the device unchangeable identification number. Here the attacker has to physically remove the GPS device from the original vehicle in order to act on its behalf. Therefore, a certified GPS device number attached with the current GPS location, velocity and direction justifies high certainty, together with other cross-verified attributes, such as the visual attributes, on the vehicle identity.

We next outline the arguments for the safety assurance implied by our scheme. The proposed approach is resistant to man-in-the-middle attack. The CA public key is conveyed to vehicles in secure settings. CA receives the request for the certificate deliverance and only the intended recipient will get the certificate $Cert$ from CA. An attempt to manipulate the certificate $Cert_S$ contents, in order to replace the attributes to fit the attacker vehicle attributes or the public key, will be detected as the digital signature $E_{PK_{CA}}(H(Attribute_S + Public\,key_S))$ yields an impossibility to modify a certificate or to produce a totally new one. Receiver R decrypts the digital signature using the CA pubic key PK_{CA} and confirms the validity. Thus, any verifiable certificate has been originated by the CA and therefore the attributes coupled with a certain public key uniquely characterize the vehicle.

After the mutual authentication is done through a signed public key verification, coupled with the fixed sense-able attributes, a session key is to be established. A random string key_r is generated at the receiver R and is sent along with the certificate $Cert_R$, in response to sender S request for certificate $Cert_R$. As the key_r can be replaced by a MitM, S needs to authenticate the origin of key_r. Moreover, an attacker can manipulate the random string in between thus, it requires to ensure the integrity. First, R encrypts the key_r and $Sequence\ Number_S$ using S public key $Public\ key_S$, i.e. $E_{Public\,key_S}(key_r + Sequence\ Number_S)$ so that only S can decrypt the random string using corresponding secret key SK_S. Thus, the confidentiality is ensured as only intended receiver can decrypt the key_r as $D_{SK_S}[E_{Public\,key_S}(key_r + Sequence\ Number_S)]$. In order to verify this key_r with the digital signature, a hashing algorithm H is applied that produces a hashed key string $H(key_r + Sequence\ Number_S)$. Second, a digital signature, i.e. $E_{Public\,key_S}(E_{SK_R}(H(key_r + Sequence\,Number_S)))$ is attached with the encrypted random string $E_{Public\,key_S}(key_r + SequenceNumber_S)$. Thus, integrity is maintained as only R can generate these signature. Similarly, only S can retrieve the $H(key_r + Sequence\ Number_S)$ from the signature using secret key SK_S and $Public\ key_R$ as $D_{SK_S}(D_{Public\,key_R}(H(key_r + Sequence\ Number_S)))$. Next, the $H(key_r + Sequence\ Number_S)$ from digital signature is compared with the hashed key string generated locally. If both hashed key strings are same then key_r is accepted as a session key. Note that the signed and encrypted key_r and $Sequence\ Number$ can not be used as part of a replay attack, however, such usage will be detected by the sender and the receiver as the actual value of key_r is not revealed to the attacker. The use of

synchronized date-time and signed association of the date-time can avoid even such unsuccessful attack attempts.

1. Sender S sends the certificate $Cert_S$=$Attributes_S$ + $Public\,key_S||E_{SK_{CA}}(H(Attributes_S + Public\,key_S))$ to a neighbor R.
2. Receiver R confirms the certificate $Cert_S$ authenticity as described in 2.(a) and then responds as detailed in 2.(b):
   (a) R verifies the digital signature using the CA public key PK_{CA}, namely, $D_{PK_{CA}}[E_{SK_{CA}}(H(Attributes_S + Public\,key_S))]$ and checks that indeed the result $H(Attributes_S + Public\,key_S)$ is equal to the hash of $Attributes_S$ and $Public\,key_S$, and then verifies $Attributes_S$ using out-of-band channels.
   (b) R responds with the certificate $Cert_R$=$Attribute_R$ + $Publickey_R||E_{SK_{CA}}(H(Attribute_R+Publickey_R))$ along with a random string key_r and certificate sequence number $Sequence\,Number_S$ encrypted with $Public\ key_S$ and digitally signed by R, i.e. $E_{Public\,key_S}(key_r + Sequence\ \ Number_S)||E_{Public\,key_S}(E_{SK_R}(H(key_r + Sequence\,Number_S)))$.
3. Sender S confirms the certificate $Cert_R$ authenticity as described in 3.(a) and then responds as detailed in 3.(b):
   (a) S verifies the digital signature using the CA public key PK_{CA}, namely, $D_{PK_{CA}}[E_{SK_{CA}}(H(Attribute_R + Public\,key_R))]$ and checks that indeed the result $H(Attribute_R + Public\,key_R)$ is equal to the hash of $Attribute_R$ and $Public\,key_R$, and then verifies $Attribute_R$ using out-of-band channels.
   (b) S decrypts the secret session key and certificate sequence number concatenated with the digital signature by using own secret key SK_S, i.e. $D_{SK_S}[E_{Public\,key_S}(key_r+SequenceNumber_S)]$ resulting into key_r. Also the digital signature of R is verified using SK_S and $Publickey_R$ respectively, i.e. $D_{SK_S}(D_{Public\,key_R}(H(key_r+Sequence\,Number_S)))$ that results into $H(key_r + Sequence\ Number_S)$. Now the hashing algorithm H is applied with $key_r + Sequence\,Number_S$ and then compared with the hashed string $H(key_r + Sequence\ Number_S)$ produced from the digital signature. If the both hash strings are same and the symmetric padded zero composition $key_r + Sequence\,Number_S$ is valid then key_r is accepted as a valid session key.
4. Sender and receiver exchange encrypted messages using key_r as a shared secret key for S and R.

Figure 2: Two rounds session key establishment

3 AKE Protocols and Out-of-Band Sensible Attributes Authentication

Many Authenticated Key Exchange protocols (AKE), that allow two parties to authenticate each other and to establish a secret key via a public communication

channel, have been proposed over the past years addressing various adversary models and possible attacks [37, 40, 36, 38, 41, 39]. Informally, as it is stated in [36], AKE protocols should guarantee the following requirements: *Authentication* – each party identifies its peer within the session; *Consistency* – if two honest parties A, B, establish a common session key K, then A believes it communicates with B, and B believes it communicates with A; *Secrecy* – if a session is established between two honest peers then no adversary should learn any information about the resultant session key.

Usually the above requirements are more formally described by detailed scenarios that involves resistance to the following attacks: *Basic KE security* is defined via so called KE experiment in which an adversary that controls a communication channel should not be able to distinguish the session key established between parties from a random value. *Forward Secrecy (FS)* property guarantees that a session key derived from a set of long-term public and private keys will not be compromised if one of the (long-term) private keys is compromised in the future. So it says that an adversary who corrupted one of the parties (learns the long-term secret key), should not be able to learn session keys of past sessions executed by that party. *Known Session Key Attack resilience* provides that an adversary who learns a session key should be unable to learn other session keys.

Additionally, authentication in AKE protocols implies resistance to various misidentification threats: *Unknown Key-Share Attacks resilience* prevents an adversary to cause the situation whereby a party (say A), after protocol completion, believes she shares a key with B, and although this is in fact the case, B mistakenly believes the key is shared with a party E (other then A). *Key Compromise Impersonation (KCI) resilience* provides that an adversary who learns a long-term secret key of some party (say A) should be unable to share a session key with A by impersonation as other party to A, although obviously it can impersonate A to any other party. *Extended Key Compromise Impersonation (E-KCI) resilience.* In regular AKE protocols parties use additional random parameters (called *ephemeral* keys), such as ephemeral Diffie-Hellman keys, coined e.g. for the purpose of session initialization. An adversary who learns both: a long-term secret key, and an ephemeral key of some party (say A), should be unable to share a session key with A by impersonation as other party to A. *Ephemeral Key Compromise Impersonation (ECI) resilience.* An adversary who learns only an ephemeral key of some party (say A) should be unable to share a session key with A by impersonation as other party to A.

In this paper we focus on specific AKE scenarios for securing the communication of vehicles via out-of-band sensible attributes. We assume that:

1. a sender and a recipient use specialized devices for recognizing out-of-band sensible attributes.
2. these devices can precisely pick the peer vehicle, and can accompany a regular (say radio communication) channel.
3. the out-of-band sensible attributes can identify a vehicle uniquely.

If the above mentioned assumptions does not hold, the protocol from Figure 2 can be a subject of impersonation repetition attacks, and does not fulfill FS feature, as it is outlined below. *Impersonation Repetition attack - version 1*: any adversary A that is within the radio range of a sender S (with $Attribute_S$) and a recipient R

(with $Attribute_R$), and that once recorded a valid transcript (including certificate of S) between them, can initialize future communication from S. Although A cannot decipher responses from R, the attack could be used to make R thinking that S wants to communicate. Moreover R can use such an initialized session to send some valid but unwanted messages to S. (see Figure 3). *Impersonation Repetition attack -*

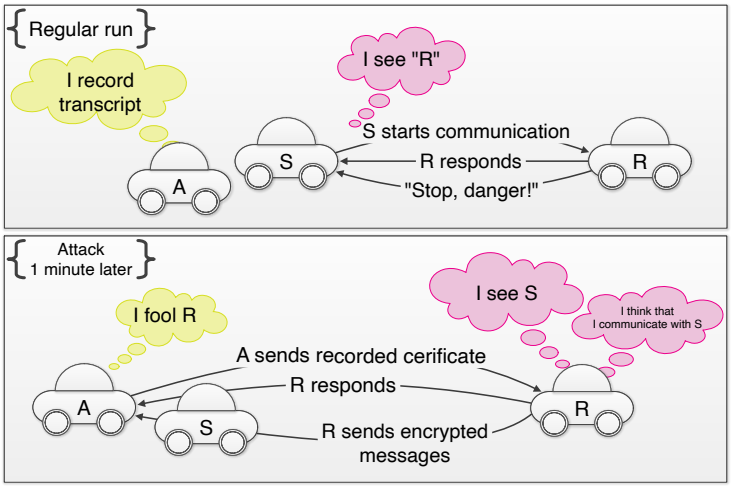

Figure 3: Repetition attack - version 1.

version 2: This attack is more powerful. An adversary A, that once recorded a valid transcript between a sender S (with $Attribute_S$) and a recipient R (with $Attribute_R$), can simulate future answers (steps 2a, 2b) for the same recipient R (or for any other recipients R' - that has similar attributes $Attribute_R$) challenged by S. Adversary A simply sends back messages previously recorded in steps 2a, 2b (see Figure 4). Thus, after S finishes protocol in accepting state, it thinks it partnered with the intended R, and starts to decrypt subsequent messages encrypted with the established key. Although, in this repetition attack, A does not learn the session key, after acquiring the first message from S the adversary A can send back previously recorded answers from R to S, finishing protocol. Subsequently A can continue with sending previously recorded ciphertexts encrypted with the previous session key. Such ciphertexts would be accepted as valid, and decrypted by S. If the protocol was run only for authentication purposes (peers do not want to communicate further, which we do not consider here), the attack itself is a serious threat, e.g. in the case where S is a police car that monitors the speed of other cars and wants to identify the recipient. *Improvements Against Impersonation Attacks.* In the case of the proposed protocol we can simply protect against impersonation attack version 1 in the following way: a sender S encrypts an acknowledgment of the second message it gets from R with the session key and sends at the beginning of the transmission through the encrypted channel. For the protection against the impersonation attack version 2 a sender S sends (in the first step) to R a concatenation $Cert_S|Nonce_S$, where $Nonce_S$ is a unique random challenge coined

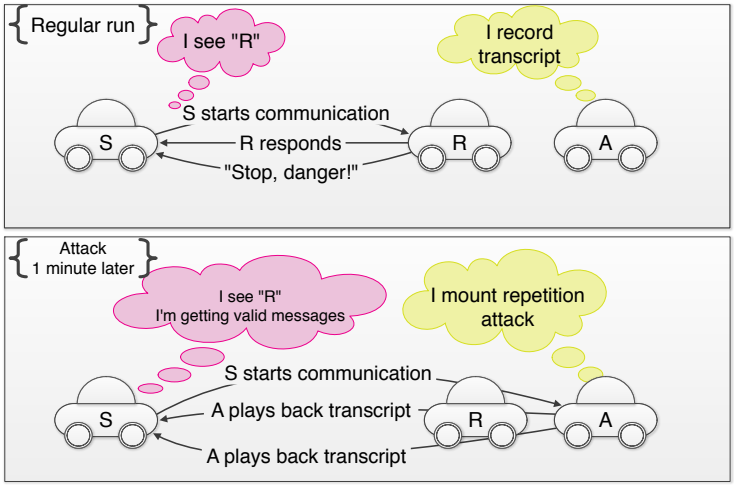

Figure 4: Repetition attack - version 2.

for that session by S. Then the cryptograms answered by R in the second step should include the same $Nounce_S$, which subsequently should be verified by S.

Forward Secrecy (FS): This is the protection of past session keys in spite of the compromise of long-term secrets. If the attacker somehow learns the long-term secret information held by a party (the party is controlled by the attacker, and referred to as corrupted), it is required that session keys, produced (and erased from memory) before the party corruption happened, will remain secure (i.e. no information on these keys should be learned by the attacker). Obviously our protocol does not fulfill FS. If the attacker records transcripts and then corrupts the party S (got its private keys), then the previous session keys key_r are exposed and transcripts can be deciphered. *Improvements for FS.* We can improve our protocol for FS by setting: $Nounce_S = g^{\alpha}$, responded $key_r = g^{\beta}$, for some random ephemeral keys α , and β. Then the session key would be derived from the value $g^{\alpha\beta}$, computed independently on both sides.

Obviously one can also utilize some three rounds protocols, instead of our two rounds protocol, protocols previously discussed in literature, that do not require a predefined knowledge of peers identity. The idea of out-of-band sense-able attributes can be incorporated into them without undermining their security. The first straightforward choice would be ISO KE protocol, described in [12], and mentioned among other protocols in [36]. Figure 5 presents the protocol, where $Cert_S$, and $Cert_R$ are certificates proposed in this paper. In the protocol, parties that receives certificates immediately validate them by the means of CA public key, and out-of-band visible attributes. They also validate received signatures and proceed only if the validation is correct. The established session key K_S, is derived from g^{xy}. Note that this protocol does not support identity hiding, as certificates are transferred in plaintexts.

If we consider anonymity (certificates should not be transferred as plaintexts) as a requested feature, we could use SIGMA-I protocol from [36] (Figure 6), where a session key K_S, an encryption key K_e and a message authentication key K_m are derived from

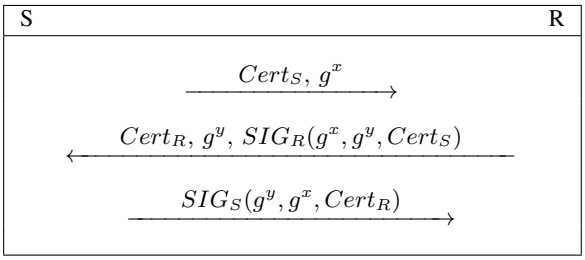

Figure 5: ISO KE adopted to the proposed certificates

g^{xy} (K_S, K_e, and K_m keys must be computationally independent from each other). Here parties decrypt messages by the means of the key K_e, validate certificates by the means of CA public key, and out-of-band visible attributes. They also validate received signatures. Each part independently proceeds only if both the decryption and validation are correct.

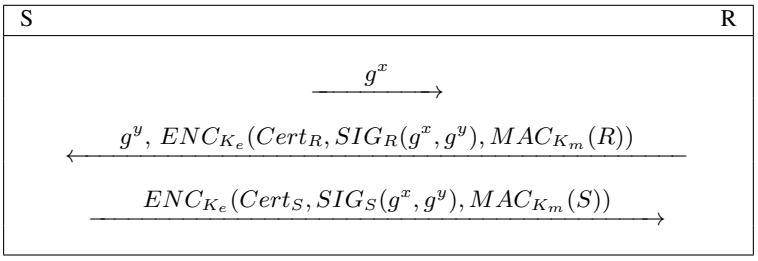

Figure 6: SIGMA-I protocol adopted to the proposed certificates

If deniability property (that assures that transcript should not be regarded as a proof of interaction) is important, then we propose to adopt one of the protocols [28, 27]. However in this case we should assume that parties private keys are discrete logarithms of corresponding public keys, and computations are performed in algebraic structures where discrete logarithm problem (DLOG) is hard. Although deniable protocols from [28, 27] require four passes of messages, they were designed for machine readable travel documents - which in turn can be implemented on smart-cards. Therefore we acknowledge that implementing them for vehicular communication can also be considered.

4 Transport Layer Security Handshake with Certified Attributes

The scheme presented in the previous section is based on Transport Layer Security (TLS) scheme augmented with the signed coupled public key and attributes. TLS handshake is based on a pre-defined sequence of phases such as mutual authentication,

random secret exchange and session key establishment. Handshake between the sender S and receiver R starts by invoking the opposite party and sending the supported range of cryptographic standards called as $Hello$ message. Mutual authentication is accomplished through the CA signed certificates called as $Certificate\ Exchange$ message. At first, S forwards the certificate $Cert_S$ to R which then verifies the CA signature on $Cert_S$ and the out-of-band sense-able fixed attributes $Attribute_S$. Similarly, S also verifies the CA signature on $Cert_R$ and the out-of-band sense-able fixed attributes $Attribute_R$.

Once the sender and receiver have exchanged and verified the respective certificates $Cert_S$, $Cert_R$ and attributes $Attribute_S$, $Attribute_R$; a session key key_r needs to be established on both sides. For that, R generates a random string key_r and shares it with S to derive a common session key between them. The random string and intended receivers certificate sequence number is encrypted $E_{Public\,key_S}(key_r + Sequence\ Number_S)$ by using the public key $Public\,key_S$ and is concatenated with a digital signature $E_{Public\,key_S}(E_{SK_R}(H(key_r + Sequence\ Number_S)))$. This way a MitM attacker can no longer fabricate the combination of session key key_r and sequence number $Sequence\ Number_S$. S can now decrypt the random string key_r with the certificate sequence number $Sequence\ Number_S$ using SK_S and also the digital signature by using SK_S and $Public\,key_R$ respectively.

This completes the discussion on mutual authentication and session key establishment. Now, S and R switches to the symmetric encryption. The recently established session key key_r is used on both sides to encrypt and decrypt the message.

5 Conclusion

The proposed work provides man-in-the-middle attack resistance and mutual authentication using certified public key and out-of-band sense-able attributes. As the CA pre-processes every vehicles public key and unchangeable attributes, there is no way that man-in-the-middle can fake the public key or the unchangeable attributes. Also, the out-of-band attributes are sense-able and can be confirmed, while moving on the road. There is no need to communicate with the CA during the real-time session key establishment of a secret key based on the mutual authentication of vehicles. The proposed approach is simple, efficient and ready to be employed in current and future vehicular networks.

Acknowledgment We thank Niv Gilboa, C. Pandu Rangan and Sree Vivek for valuable comments.

References

1. VANET Projects and Consortia available at URL: http://www.vanet.info/?q=node/13.
2. CAR 2 CAR Communication Consortium (C2C-CC) available at URL: http://www.car-to-car.org/.
3. Cartalk2000 available at URL: http://www.cartalk2000.net/.
4. Network on Wheels (NoW) available at URL: http://www.network-on-wheels.de/.

5. Vehicle Infrastructure Integration (VII) available at URL: http://www.vehicle-infrastructure.org/.
6. Partners for Advanced Transportation TecHnology (PATH) available at URL: http://www.path.berkeley.edu/.
7. Secure Vehicle Communication (SeVeCom) available at URL: http://www.sevecom.org/.
8. E-safety Vehicle Intrusion protected Applications (EVITA) available at URL: http://www.evita-project.org/.
9. Dedicated Short Range Communications (DSRC) Concept of Operations and ISO Layer Implementation Summary available at URL: http://grouper.ieee.org/groups/scc32/Attachments.html.
10. Global System for Mobile Communications (GSM) available at URL: http://www.etsi.org/index.php/ technologies-clusters/technologies/mobile/gsm.
11. International Organization for Standardization (ISO) available at URL: http://www.iso.org/.
12. Iso/iec is 9798-3, entity authentication mechanisms, part 3: Entity authentication using asymmetric techniques, 1993.
13. 2005.
14. 2010.
15. O. Abumansoor and A. Boukerche. Preventing a dos threat in vehicular ad-hoc networks using adaptive group beaconing. In *Proceedings of the 8h ACM symposium on QoS and security for wireless and mobile networks*, pages 63–70, New York, NY, USA, 2012.
16. M. Barbeau, J. Hall, and E. Kranakis. Detecting impersonation attacks in future wireless and mobile networks. In *MADNES*, pages 80–95, 2005.
17. C. Boyd and J. Nieto. On forward secrecy in one-round key exchange. In L. Chen, editor, *Cryptography and Coding*, volume 7089 of *Lecture Notes in Computer Science*, pages 451–468. Springer Berlin Heidelberg, 2011.
18. M. Cagalj, S. Capkun, and J.-P. Hubaux. Key agreement in peer-to-peer wireless networks. *Proceedings of the IEEE*, pages 467–478, 2006.
19. C. Campolo and A. Molinaro. Multichannel communications in vehicular ad-hoc networks: A survey. *Communications Magazine, IEEE*, 2013.
20. 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.*, pages 208–223, 2008.
21. G. Chandrasekaran, J. Francisco, V. Ganapathy, M. Gruteser, and W. Trappe. Detecting identity spoofs in ieee 802.11e wireless networks. In *Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE*, pages 1–6, 2009.
22. Z. Chen, S. Guo, K. Zheng, and H. Li. Research on man-in-the-middle denial of service attack in sip voip. In *Proceedings of the 2009 International Conference on Networks Security, Wireless Communications and Trusted Computing - Volume 02*, pages 263–266, Washington, DC, USA, 2009.
23. L. C. C. Desmond, C. C. Yuan, T. C. Pheng, and R. S. Lee. Identifying unique devices through wireless fingerprinting. In *Proceedings of the first ACM conference on Wireless network security*, pages 46–55, New York, NY, USA, 2008.
24. W. Diffie and M. Hellman. New directions in cryptography. *IEEE Trans. Inf. Theor.*, pages 644–654, 2006.
25. M. Gerla and L. Kleinrock. Vehicular networks and the future of the mobile internet. *Computer Networks*, pages 457–469, 2011.
26. M. Goodrich, M. Sirivianos, J. Solis, G. Tsudik, and E. Uzun. Loud and clear: Human-verifiable authentication based on audio. In *Distributed Computing Systems, 2006. ICDCS 2006. 26th IEEE International Conference on*, page 10, 2006.

27. L. Hanzlik, K. Kluczniak, L. Krzywiecki, and M. Kutylowski. Mutual chip authentication. Proceedings, 3rd IEEE International Symposium on Anonymity and Communication Systems 2013, 2013.
28. L. Hanzlik, K. Kluczniak, L. Krzywiecki, and M. Kutylowski. Mutual restricted identification. Proceedings, Euro PKI 2013, 2013.
29. J. Harri, F. Filali, and C. Bonnet. Mobility models for vehicular ad-hoc networks: A survey and taxonomy. *Communications Surveys Tutorials, IEEE*, pages 19–41, 2009.
30. L. Holmquist, F. Mattern, B. Schiele, P. Alahuhta, M. Beigl5, and H.-W. Gellersen. Smart-its friends: A technique for users to easily establish connections between smart artefacts. In *Ubicomp 2001: Ubiquitous Computing*, pages 116–122. 2001.
31. 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.*, pages 775–793, 2010.
32. I. R. Jeong, J. Katz, and D. H. Lee. One-round protocols for two-party authenticated key exchange. In *ACNS*, 2004.
33. D. Kgler. man in the middle attacks on bluetooth. In *Financial Cryptography*, pages 149–161. 2003.
34. B. Komu, M. Mzyece, and K. Djouani. Spin-based verification of authentication protocols in wimax networks. In *Vehicular Technology Conference (VTC Fall), 2012 IEEE*, pages 1–5, 2012.
35. 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 *Security and Privacy (SP), 2010 IEEE Symposium on*, pages 447–462, 2010.
36. H. Krawczyk. Sigma: The 'sign-and-mac' approach to authenticated Diffie-Hellman and its use in the ike-protocols. In D. Boneh, editor, *CRYPTO*, volume 2729 of *LNCS*, pages 400–425. Springer, 2003.
37. H. Krawczyk. HMQV: A high-performance secure Diffie-Hellman protocol. Cryptology ePrint Archive, Report 2005/176, 2005.
38. B. A. LaMacchia, K. Lauter, and A. Mityagin. Stronger security of authenticated key exchange. In W. Susilo, J. K. Liu, and Y. Mu, editors, *ProvSec*, volume 4784 of *LNCS*, pages 1–16. Springer, 2007.
39. K. Lauter and A. Mityagin. Security analysis of kea authenticated key exchange protocol. In M. Yung, Y. Dodis, A. Kiayias, and T. Malkin, editors, *Public Key Cryptography*, volume 3958 of *LNCS*, pages 378–394. Springer, 2006.
40. L. Law, A. Menezes, M. Qu, J. Solinas, and S. Vanstone. An efficient protocol for authenticated key agreement. *Designs, Codes and Cryptography*, 28(2):119–134, 2003.
41. J. Lee and J. H. Park. Authenticated key exchange secure under the computational Diffie-Hellman assumption. Cryptology ePrint Archive, Report 2008/344, 2008.
42. D. Martins and H. Guyennet. Wireless sensor network attacks and security mechanisms: A short survey. In *Network-Based Information Systems (NBiS), 2010 13th International Conference on*, pages 313–320, 2010.
43. R. Mayrhofer and H. Gellersen. Spontaneous mobile device authentication based on sensor data. *Information Security Technical Report*.
44. R. Mayrhofer and H. Gellersen. Shake well before use: Authentication based on accelerometer data. In *Pervasive Computing*, pages 144–161. 2007.
45. 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*, pages 110–124, 2005.
46. P. Nagrath and B. Gupta. Wormhole attacks in wireless ad-hoc networks and their counter measurements: A survey. In *Electronics Computer Technology (ICECT), 2011 3rd International Conference on*, pages 245–250, 2011.

47. R. Oppliger. Certification authorities under attack: A plea for certificate legitimation. *Internet Computing, IEEE*, page 1, 2013.
48. 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*, pages 100–109, 2008.
49. A. Perrig, R. Canetti, J. D. Tygar, and D. Song. The tesla broadcast authentication protocol, 2002.
50. R. Prasad and N. Saxena. Efficient device pairing using human-comparable synchronized audiovisual patterns. In *Applied Cryptography and Network Security*, pages 328–345. 2008.
51. M. Raya and J.-P. Hubaux. The security of vanets. In *Proceedings of the 2nd ACM international workshop on Vehicular ad hoc networks*, pages 93–94, New York, NY, USA, 2005.
52. M. Raya and J.-P. Hubaux. Securing vehicular ad-hoc networks. *Journal of Computer Security*, pages 39–68, 2007.
53. X. Ren and X.-W. Wu. A novel dynamic user authentication scheme. In *Communications and Information Technologies (ISCIT), 2012 International Symposium on*, pages 713–717, 2012.
54. R. L. Rivest and A. Shamir. How to expose an eavesdropper. *Commun. ACM*, pages 393–394, 1984.
55. N. Saxena, J.-E. Ekberg, K. Kostiainen, and N. Asokan. Secure device pairing based on a visual channel. In *Security and Privacy, 2006 IEEE Symposium on*, page 6, 2006.
56. K. A. Scarfone, D. Dicoi, M. Sexton, and C. Tibbs. Sp 800-48 rev. 1. guide to securing legacy ieee 802.11 wireless networks. Technical report, Gaithersburg, MD, United States, 2008.
57. D. B. Smetters, D. Balfanz, D. K. Smetters, P. Stewart, and H. C. Wong. Talking to strangers: Authentication in ad-hoc wireless networks. 2002.
58. F. Stajano and R. Anderson. The resurrecting duckling: Security issues for ubiquitous computing. *Computer*, pages 22–26, 2002.
59. A. Studer, F. Bai, B. Bellur, and A. Perrig. Flexible, extensible, and efficient vanet authentication. *Communications and Networks, Journal of*, pages 574–588, 2009.
60. J.-K. Tsay and S. Mjlsnes. A vulnerability in the umts and lte authentication and key agreement protocols. In *Computer Network Security*, pages 65–76. 2012.
61. N.-W. Wang, Y.-M. Huang, and W.-M. Chen. A novel secure communication scheme in vehicular ad-hoc networks. *Comput. Commun.*, pages 2827–2837, 2008.
62. Y. Xiao, S. Sethi, H.-H. Chen, and B. Sun. Security services and enhancements in the ieee 802.15.4 wireless sensor networks. In *Global Telecommunications Conference, 2005. GLOBECOM '05. IEEE*, page 5, 2005.
63. L. Zhang, W. Jia, S. Wen, and D. Yao. A man-in-the-middle attack on 3g-wlan interworking. In *Proceedings of the 2010 International Conference on Communications and Mobile Computing - Volume 01*, pages 121–125, Washington, DC, USA, 2010.