
(doi: 10.1109/IV51971.2022.9827444)

This is the Author Accepted Manuscript.

© 2022 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.

There may be differences between this version and the published version. You are advised to consult the publisher’s version if you wish to cite from it.

http://eprints.gla.ac.uk/269001/

Deposited on: 12 April 2022
Cross-Layer Authentication based on Physical-Layer Signatures for Secure Vehicular Communication

Mahmoud A. Shawky†, Qammar H. Abbasi‡, Muhammad Ali Imran†, Shuja Ansari†, and Ahmad Taha†

Abstract—In recent years, research has focused on exploiting the inherent physical (PHY) characteristics of wireless channels to discriminate between different spatially separated network terminals, mitigating the significant costs of signature-based techniques. In this paper, the legitimacy of the corresponding terminal is firstly verified at the protocol stack’s upper layers, and then the re-authentication process is performed at the PHY-layer. In the latter, a unique PHY-layer signature is created for each transmission based on the spatially and temporally correlated channel attributes. Extensive simulation has shown the capability of the proposed scheme to support high detection probability at small signal-to-noise ratios. In addition, security evaluation is conducted against passive and active attacks. Moreover, computation and communication comparisons are performed to demonstrate that the proposed scheme provides superior performance compared to conventional cryptographic approaches.


I. INTRODUCTION

Intelligent Transportation Systems are employed to facilitate direct connectivity between vehicles, pedestrians, and roadside infrastructures referred to as vehicular communication. By using wireless channels for communication between terminals, vehicular networks are susceptible to a wide range of attacks, such as impersonation, modification, and replay attacks [1]. Therefore, message authentication and integrity are crucial security services that must be assured to avoid these attacks. Most of the existing authentication schemes have been developed based on the difficulty of solving complex cryptographic problems, e.g., discrete logarithm and factorization problems [2]. However, the significant computational cost of the mathematical crypto operations limits the number of the communicating terminals in the network [3]. In response, researchers have come up with several solutions to this problem, including singular and bilinear batch verifications and using proxy vehicles to verify signatures on behalf of endpoint terminals [4-6]. Generally, the vehicular network structure consists of the trusted authority (TA), roadside units (RSUs), and vehicles’ onboard units (OBUs).

Recently, many physical (PHY) layer discrimination techniques have been introduced to the research community as a promising solution to the significant costs of traditional signature-based schemes. Some of these techniques exploit the wireless channel reciprocity and randomness to ensure that the receiver is still in communication with the same transmitter [7-8]. These techniques are referred to as “feature tracking”. Hardware imperfections attributes are also utilized to construct a radio frequency fingerprint for each terminal in the network [9-10]. However, these approaches demonstrated low reliability due to the signal quality fluctuation caused by the limited range of communication devices as well as the significant variations of channel attributes over time. Therefore, key-based PHY-layer authentication has been proposed as an alternative solution that requires a pre-agreed key for successful detection [11-12]. Nowadays, cross-layer authentication has emerged by integrating PHY-layer techniques with upper layers cryptographic signatures. However, choosing the proper PHY-layer technique must be compatible with the application’s requirements in terms of computational resources availability, communication range, and number of network terminals.

In [13], a cross-layer scheme has been patented by integrating the Public Key Infrastructure (PKI) based authentication with RF fingerprinting for re-authentication. In fact, the small dissimilarities between the extracted features from different devices can mislead the decision rule, which cannot support high scalability. In [14-15], the integration is performed with feature tracking techniques. However, an extensive observation is essential to extract terminals’ distinctive features for successful detection, in addition to the low detection probability at small signal-to-noise ratios. Reference [16] integrated the physically unclonable functions of the integrated circuits with a pseudo-identity signature-based algorithm. Unfortunately, the instability of these features due to voltage supply variations and electromagnetic interference constitutes a complex challenge. In summary, some of the mentioned works are applicable in resource-constrained applications. However, it is not applicable in long-range and high-speed dynamic terminals, e.g., vehicular communication. To address this gap, the proposed scheme in this paper uses PKI-based algorithm for initial identity verification followed by creating a PHY-layer orthogonal frequency division multiplexing (OFDM) signature for each subsequent transmission. This signature is considered as a PHY-layer message authentication code for the attached data packet that can only be equalized at the intended endpoint terminal.

The remainder of this paper is organized as follows. Section II describes the proposed scheme’s structure. In Section III, threat modelling is discussed, while Section IV presents simulation results and comparisons. Finally, Section V concludes the current study.
II. CROSS-LAYER AUTHENTICATION SCHEME

In this section, the proposed scheme is firstly modelled, and then, in the following subsections, the scheme is discussed in detail.

A. Scheme modelling

The proposed scheme aims to authenticate the sender’s identity and verify the message’s integrity with minimum computation and communication costs. For vehicle-to-vehicle (V2V) communication, if $V_i$ is in the transmission range of $V_j$ and wants to initiate a trust connection, the authentication is carried out in a two-step process, as illustrated in Fig. 1, and explained below:

S1. During the first transmission slot, the corresponding terminal’s legitimacy is initially verified using a signature-based authentication algorithm executed at the upper layers of the protocol stack.

S2. If the mutual verification succeeds, the re-authentication process is performed by generating a PHY-layer signature to the attached data packet, which is used to identify the message integrity. Otherwise, the initial verification step (S1) is aborted.

The generated PHY-layer signature can only be equalized at the side of the intended receiver based on the spatial and temporal correlation of channel responses between two communicating terminals within the coherence time interval $T_c$. For longer V2V communication distances, intermediate cooperative relays can also be employed to amplify and forward (AF) the received data packets, including the attached PHY-layer signatures. Table I lists the notations used in this paper.

B. Signature-based authentication algorithm

In this algorithm, each terminal verifies the legitimacy of the corresponding vehicle and generates a symmetric session key. In fact, the mutual authentication process consists of three primary phases.

S1.1. System initialisation phase: TA computes the algorithm’s public parameters $PPs$ as follows.

- Selecting at random two prime numbers $p$ and $q$ are used to generate the cyclic additive group $G$ of the elliptic curve $E: x^3 + ax + b$ mod $q$ based on the basepoint $P$ so that $a, b \in \text{Finite Field}(p)$ and $\Delta = 4a^3 + 27b^2 \neq 0$.
- Choosing the hash function $H_i: [0, 1]^* \rightarrow [0, 1]^N_1$.
- Randomly selecting TA’s secret key $\beta \in Z_p^*$.

S1.2. System registration phase: For each registered vehicle $V_i$, TA has to do the following steps.

- TA creates a list of vehicle’s anonymous certificates $[\text{Cert}_1, ..., \text{Cert}_z]$ by randomly selecting an array of secret keys $[sk_1, ..., sk_z] \in Z_q$ used to compute their corresponding public keys $[pk_1, ..., pk_z]$ for $pk_i = sk_i \cdot P$ and $i = 1, ..., z$. For privacy preservation, all $V_i$’s certificates are generated with different pseudo-identities $PIDV_i \in [0, 1]^*$ to preserve $V_i$’s real identity from exposure. Next, TA computes certificate signatures $[\sigma_{TA1}, ..., \sigma_{TAD}]$ for $\sigma_{TAi} = sign(H_i,(pk_i \parallel PIDV_i \parallel Tp_i)_{\beta})$ where $T_p$ is the certificate expiry date. Finally, a single certificate $\text{Cert}_i$ can be represented by the tuple $(PIDV_i, pk_i, Tp_i, \sigma_{TAi})$.
- TA preloads a list of the generated certificates, their related secret keys $[sk_1, ..., sk_z]$, and the public parameters $PPs = \langle p, q, G, P, a, b, H_i \rangle$ into the $V_i$’s OBU.

S1.3. Identity verification phase: For secure communication between $V_i$ and $V_j$, the following identification substeps must be executed:

S1.3.1. $V_i$ picks up a certificate at random $\text{Cert}_{V_i} = (PIDV_i, pk_{V_i}, T_{V_i}, \sigma_{TA})$ and its related secret key $sk_{V_i}$, then signs the hashed $\text{Cert}_{V_i}$ at the $T_1$ timestamp using $sk_{V_i}$ so that the generated signature can be expressed as $\sigma_{V_i} = sign(H_i(\text{Cert}_{V_i} \parallel T_{V_i}))_{sk_{V_i}}$. Finally, $V_i$ sends the tuple $(\text{Cert}_{V_i}, T_1, \sigma_{V_i})$ to $V_j$.

S1.3.2. $V_j$ uses the certified public key to verify the received signature $ver(\sigma_{V_i}, pk_{V_i})$, checks the freshness of the received timestamp $T_1$ to avoid replaying attacks, identifies the legitimacy of $V_i$ by testing whether if $\text{Cert}_{V_i}$ is in the certificate revocation list (CRL), and stores $V_i$’s $\text{Cert}_{V_i}$. The same process of signature generation is performed at the side of vehicle $V_j$ by picking up at random $\text{Cert}_{V_j} = (PIDV_j, pk_{V_j}, T_{V_j}, \sigma_{TA})$ and its related secret key $sk_{V_j}$, computing the session key $sk_{V_{ij}} = sk_{V_i} \cdot pk_{V_j}$ and $V_j$’s signature $\sigma_{V_j} = sign(H_j(\text{Cert}_{V_j} \parallel T_{V_j}))$ at the $T_2$ timestamp. Finally, $V_j$ sends the tuple $(\text{Cert}_{V_j}, T_2, \sigma_{V_j})$ to $V_i$.

S1.3.3. $V_i$ in turn verifies the received signature, checks the freshness of $T_2$, tests whether if $\text{Cert}_{V_j}$ is in the CRL, and then computes the session key $sk_{V_{ij}} = sk_{V_i} \cdot pk_{V_j}$.

Fig. 2 presents the identity authentication phase structure. This process is frequently updated with different $\text{Cert}_{V_i}$ and $\text{Cert}_{V_j}$ to avoid location tracking attacks [1].

![Flowchart of the proposed cross-layer scheme.](image)

**Table I**

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>$PPs$</td>
<td>Scheme’s public parameters</td>
</tr>
<tr>
<td>$\beta$</td>
<td>The system’s master key</td>
</tr>
<tr>
<td>$sk_{V_i}$</td>
<td>The secret key of vehicle $V_i$</td>
</tr>
<tr>
<td>$pk_{V_i}$</td>
<td>Public key of vehicle $V_i$</td>
</tr>
<tr>
<td>$sk_{V_{ij}}$</td>
<td>The symmetric session key between vehicles $V_i$ and $V_j$</td>
</tr>
<tr>
<td>$Cert_{V_i}$</td>
<td>Digital public key certificate of vehicle $V_i$</td>
</tr>
<tr>
<td>$T_{V_i}$</td>
<td>Certificate expiry date in the order of a few minutes</td>
</tr>
<tr>
<td>$\sigma_{TA}$</td>
<td>The generated signature by the trusted authority (TA)</td>
</tr>
<tr>
<td>$\sigma_{V_i}$</td>
<td>The generated signature by vehicle $V_i$</td>
</tr>
<tr>
<td>$PIDV_i$</td>
<td>Pseudo-identity of vehicle $V_i$</td>
</tr>
<tr>
<td>$T_{V_i}$</td>
<td>The timestamp of the generated signature</td>
</tr>
<tr>
<td>$H_1, H_2$</td>
<td>One-way hash functions</td>
</tr>
<tr>
<td>$\phi_a, \phi_b$</td>
<td>The mapped signatures</td>
</tr>
<tr>
<td>$MC(i)$</td>
<td>Mapping operation</td>
</tr>
<tr>
<td>${sk_{V_{ij}}}_{1, 2}$</td>
<td>The $x$ and $y$ coordinates for the point $sk_{V_{ij}} \in \mathbb{G}$</td>
</tr>
<tr>
<td>$\tau$</td>
<td>Threshold value</td>
</tr>
</tbody>
</table>
C. PHY-Layer Re-authentication Algorithm

In this section, and after identifying the legitimacy of the corresponding terminal, the re-authentication process is presented in detail for OFDM system of N subcarriers, with all formulae expressed in the frequency domain. The computed session subcarrier $s_{kV_i,j} \in \mathcal{G}$ is used for generating the preliminary keys $\{k_a, k_b\}$ for $k_a = \{s_{kV_i,j}\}$ and $k_b = \{s_{kV_i,j}\}$. These sub-keys are used for generating the PHY-layer signature of the subsequent data packets, employing AF cooperative relaying between both terminals as shown in Fig. 3. Generally, the re-authentication step comprises three phases, i.e., system initialisation, PHY-layer signature generation, and verification.

S2.1. System initialisation phase: TA is also responsible for initialising the PHY-layer system public parameters as a part of the PPs presented in the signature-based algorithm.

- Mapping operation: $M(X) \rightarrow Y$ is a 2-bits mapping operation that maps the input variable $X = \{x_1, x_2, \ldots, x_{2N-1}, x_{2N}\}$ of length $|X| = 2N$ bits to generate $Y$ as
  \[
  Y_i = M(X_i) = \begin{cases} 
  0 & x_i = [0] \\
  1 & x_i = [1] \\
  3 & x_i = [2] \\
  5 & x_i = [3] 
  \end{cases} \quad \text{for } i = 1, \ldots, N
  \]
- Choosing the hash function $H_2: \{0, 1\}^* \rightarrow \{0, 1\}^{2N}$.
- Preloading the tuple $(H_2, M(\cdot))$ into vehicles’ OBUs during the registration phase.

S2.2. PHY-layer signature generation phase: Let us consider $V_i(Alice)$ wants to send a safety-related message $m$ to $V_j(Bob)$ within the same region. In that case, the PHY-layer signature generation process is performed through two main stages as follows.

1) Signature preparation stage: $V_i$ generates the signature of the hashed tuple $(PID_{V_i}, T_3, m)$ by estimating $\phi_a$ and $\phi_b$, in which $\phi_a = M(H_2(k_a \| m \| PID_{V_i} \| T_3))$ and $\phi_b = M(H_2(k_b \| m \| PID_{V_i} \| T_3))$ are created at $T_3$ timestamp.

2) OFDM symbols initialisation stage: In this stage, two subsequent OFDM symbols are initiated by $V_i$ at two subsequent time slots $t_0$ and $t_0 + \Delta t$ for $\Delta t < T_3$ with random phases $\theta_i$ uniformly distributed over $[0, 2\pi]$ and the mapped signatures $\phi_a$ and $\phi_b$. The generated signals of the $i^{th}$ subcarrier can be formulated as
  \[
  s_{ai}(t_0 + \Delta t) = \exp(j(\theta_i + \phi_{a,i}))
  \]

where $i$ ranges from 1 to $N$. Finally, the tuple $(PID_{V_i}, T_3, m)$ is concatenated with the generated OFDM symbols and sent to $V_j$. The transmission can be done directly or through $R$ intermediate cooperative relays using amplify and forward technique.

S2.3. PHY-layer signature verification phase: The received symbols by $V_j$ at time $t_1$ and $t_1 + \Delta t$ can be formulated in a noiseless channel as
  \[
  r_{bj}(t_1) = \Pi_{R}[h_{R,i}] \exp(j(\theta_i + \phi_{b,i} + \sum_R \xi_{R,i})) \quad (4)
  \]
  \[
  r_{bj}(t_1 + \Delta t) = \Pi_{R}[h_{R,i}] \exp(j(\theta_i + \phi_{b,i} + \sum_R \xi_{R,i})) \quad (5)
  \]
where $\Pi_{R}[h_{R,i}]$ and $\sum_R \xi_{R,i}$ are the $i^{th}$ subcarrier fading coefficient and the channel-phase response between legitimate communication nodes, passing through a number of $R$ intermediate terminals. In the same coherence interval, channel attributes between both terminals are correlated. Thus, the channel responses $(h_{R,i}(t_1), \xi_{R,i}(t_1))$ and $(h_{R,i}(t_1 + \Delta t), \xi_{R,i}(t_1 + \Delta t))$ are highly correlated for $\Delta t < T_c$. The received signals of equations (4) and (5) can only be equalized at the side of $V_j$ based on the symmetric session key $s_{kV_j,-j}$ and the received tuple $(PID_{V_j}, T_3, m)$ according to the following stages.

1) Signature equalization stage: $V_j$ computes $\hat{\phi}_a = M(H_2(k_a \| m \| PID_{V_j} \| T_3))$ and $\hat{\phi}_b = M(H_2(k_b \| m \| PID_{V_j} \| T_3))$. Then, $V_j$ equalizes the received signals as
  \[
  c_{1,j}(t_1) = r_{bj}(t_1) \exp(-j(\hat{\phi}_{a,i})) = \Pi_{R}[h_{R,i}] \exp(j(\theta_i + \phi_{a,i} - \hat{\phi}_{a,i} + \sum_R \xi_{R,i})) = \Pi_{R}[h_{R,i}] \exp(j(\theta_i + \sum_R \xi_{R,i})) \quad (6)
  \]
  \[
  c_{2,j}(t_1 + \Delta t) = r_{bj}(t_1 + \Delta t) \exp(-j(\hat{\phi}_{b,i})) \quad \text{as}
  \]
  \[
  c_{2,j}(t_1 + \Delta t) = r_{bj}(t_1 + \Delta t) \exp(-j(\hat{\phi}_{b,i})) = \Pi_{R}[h_{R,i}] \exp(j(\theta_i + \phi_{b,i} - \hat{\phi}_{b,i} + \sum_R \xi_{R,i})) = \Pi_{R}[h_{R,i}] \exp(j(\theta_i + \sum_R \xi_{R,i})) \quad (7)
  \]
2) Signature verification stage: $V_j$ checks the freshness of the received timestamp $T_3$, then verifies the integrity of the received message by computing the circular variance [17] $\text{Var}(\cdot)$ of $c_i(t) = c_{1,i}(t) c_{2,i}(t_1 + \Delta t)$ as
  \[
  v = \text{Var}(\sum_{i=1}^{N} c_{1,i}(t) c_{2,i}(t_1 + \Delta t)) \quad (8)
  \]
Suppose a third party $V_k(Eve)$ is trying to impersonate $V_i$ or modify the message contents. In that case, it is considered that Eve initiated a different key $K_e$ for the signature generation stage which can be represented as a binary hypothesis testing problem as:
\[ v \leq \tau, \text{ for } \begin{cases} H_0: & \hat{\theta}_a = \theta_a & \hat{\theta}_b = \theta_b \\ H_1: & \hat{\theta}_a = \theta_a & \hat{\theta}_b = \theta_b \end{cases} \]  

(9)

Taking the value \( v \) in comparison with the threshold value \( \tau \) leads to the final decision (\( H_0 \) denotes Alice is authenticated as a legitimate terminal, otherwise \( H_1 \)).

### III. Threat Modelling

Eve acts as an attacker who is familiar with the network configuration and scheme structure. However, she is unaware of the symmetric session key \( sk_{V_{i-j}} \) between legitimate parties, Alice and Bob. Considering Eve as a passive attacker who eavesdrops on the transmitted PHY-layer signatures and tries to derive the correct sub-keys, it is hard for Eve to differentiate between the mapped signatures \( \phi_a \) and \( \phi_b \) and random phases \( \theta_i \). Thus, Eve is considered to be an active adversary who is capable of executing three primary attacks as follows.

1) **Impersonation attack**: In this attack, Eve is trying to impersonate Alice to generate a correct PHY-layer signature. However, she cannot generate a correct estimation due to her unawareness of the authentic key.

2) **Replay attack**: In this attack, Eve attempts to retransmit a previously sent message by Alice. However, the recipient checks the freshness of each received signature based on the attached timestamp \( T_3 \), making such an attack easy to detect.

3) **Modification attack**: In this attack, Eve alters Alice’s message content and returns it to Bob. In contrast, she cannot compute the correct PHY-layer signature related to the altered message due to her unawareness about \( sk_{V_{i-j}} \).

### IV. Performance Evaluation

In this section, the effectiveness of the proposed scheme is evaluated based on simulation analysis, and then a comparison of computation and communication costs is presented.

#### A. Simulation analysis

The probability density functions (PDFs) are evaluated at different signal-to-noise ratios (SNRs) in order to determine the detection probability \( P_d \) under different false alarm values \( P_f \). An extensive Monte-Carlo simulation is conducted to obtain accurate estimates of the PDFs. Since \( v \) in equation (8) is the circular variance of \( N \) samples, \( v \) is subject to the central limit theorem and can be approximated as a normally distributed random variable with means and variances \( \mu_{H_01} \) and \( \sigma_{H_01} \), respectively, as shown in Fig. 4. The PDFs for both hypotheses are ideally separated, allowing the determination of the proper threshold value \( \tau \).

In order to evaluate the performance of the proposed algorithm, the receiver operating characteristics (ROCs; \( P_d \) versus \( P_f \)) are evaluated at different SNR values \([5, 0, -2, -5]\) dB, as illustrated in Fig. 5. It can be noted that high \( P_d \geq 0.9 \) is obtained for end-to-end direct transmission at small SNR up to \(-2\) dB and acceptable \( P_f \leq 0.1 \). In Fig. 6, the ROCs are estimated for different numbers of \( R \) intermediate relays at SNR = 5 dB. This implies that increasing the number of relays reduces the ROCs. However, this can support V2V communication for longer distances. For higher performance and hence the PDFs obey the central limit theorem, a higher number of subcarriers could be considered, leading to high \( P_d \) at very small SNR values (-5 dB), as demonstrated in Fig. 7.

#### B. Computation and Communication Overheads

In this part, comparisons of computation and communication costs of verifying and transmitting \( n \) signatures are tabulated in II. In Table II, \( T_{m}, T_{g}, T_{b}, T_{M-n}, T_{M} \), and \( T_{M} \) are the time required for executing a scalar multiplication, bilinear pairing, hash function, map-to-point hash function, and mapping operation, respectively. The computational cost of the verification process is evaluated for the overall scheme to be \([ T_{m} + n(2T_b + 2T_{M}) ] \) in which \( T_{m} \) is the time needed to generate the shared session key at the first time slot, while \([2T_b + 2T_{M}] \) is the consumed time for verifying \( n \) subsequent received PHY-layer signatures. The communication cost is \([1184 + n(2N + 192)] \) bits, assuming the size of the transmitted tuple \((s_{vec}, T_r, \sigma_{vec}) = 832 + 32 + 320 = 1184 \) bits for the first transmission and \([2N + 192] \) bits for the PHY-layer signature of length 2\( N \) and \((PID_{V_r}, T_r) = 160 + 32 = 192 \) bits at the subsequent \( n \) transmissions.
Fig. 5. ROCs at different SNR values and R = 0 Relays.

Fig. 6. ROCs at SNR = 5 dB and different number of Relays.

Fig. 7. ROCs at SNR = -5 dB, R = 0 Relays and different N subcarriers.

Fig. 8 shows the computation and communication costs of verifying and transmitting 1000 signatures from a single vehicle. It can be noted that the proposed scheme can save [77%, 94%] computation and [64%, 37%] communication costs compared to CPPA [4] and NERA [5], respectively.

V. CONCLUSIONS

This paper exploits the inherent wireless channel properties to create a PHY-layer OFDM signature that functions as an alternative to the traditional cryptographic signatures, reducing the considerable signalling and computation overheads of PKI-based approaches. Extensive simulations proved that the proposed scheme is effective and can provide a high authentication rate at small SNR values. In addition, we carefully evaluated the immunity of this work against possible passive and active attacks, thus proving that the novel algorithm successfully ensures the integrity of message contents. Furthermore, comparisons are made in terms of computation and communication costs to prove that the proposed scheme can save significant costs compared to conventional techniques. In future work, a PHY-layer secret key extraction algorithm such as [18] could be used to create a dynamic PHY-layer signature using the extracted location-dependent shared key.

REFERENCES


