Joint Localization-based Node Authentication and Secret Key Generation

Muralikrishnan Srinivasan, Sotiris Skaperas, Mahdi Shakiba Herfeh, Arsenia Chorti

Joint Localization-based Node Authentication and Secret Key Generation

Muralikrishnan Srinivasan[1], Sotiris Skaperas[2], Mahdi Shakiba Herfeh[2], and Arsenia Chorti[2]

***Abstract*—In this paper, we devise preprocessing schemes to disentangle channel state information (CSI) into predictable and unpredictable components to simultaneously provide two cornerstone security operations. The predictable components are used for node authentication and the unpredictable components for secret key generation (SKG). For the case of SKG, to prevent Eve from exploiting potential spatial, frequency or time correlations with the legitimate users, which would reduce the effective key space through a decrease in the brute force attack size, in this work, we emphasise the need for reducing the spatial correlation (SC) at different transmitter locations. We also study the trade-off between SC and reconciliation in the uplink and the downlink. Furthermore, we discuss the importance of a more robust criterion - independence - over decorrelation between the legitimate users and eavesdroppers. Finally, we propose a metric for quantifying uniqueness in the predictable components for node authentication, using the total variation distance (TVD).**

I. Introduction

Sixth-generation (6G) systems such as massive Internet of Things (IoT) networks will have an extensive range of delay and latency constraints, as well as computational, power and energy limitations. Securing future networks under such a broad spectrum of non-functional requirements can be challenging [1]. In addition, further developments that will increase the attack surface of 6G systems are the extensive introduction of artificial intelligence (AI) and machine learning (ML) and the rapid advances in quantum computing [2], [3].

On the other hand, the wireless channel between two legitimate users is intrinsic to the users' environment and is affected by users' movements or scatterers. Since the characteristics of the wireless medium between two users are both location-based and random, the channel impulse response can be exploited to generate keys for authentication while any particular channel realization can be used as an entropy source for confidentiality (e.g., by generating keys that are used with symmetric block cyphers) [4]–[6].

Building on this premise, in this work, we view the wireless fading coefficients as consisting of two parts, namely a predictable part (large scale fading including path loss and shadowing) and an unpredictable part (small scale fading) [7]. The path loss is deterministic (i.e., location-based) and, therefore, useful for authentication purposes, e.g., using localization information in multi-factor authentication protocols [8], while shadowing exhibits high correlation in time/frequency/space. On the contrary, the small-scale fading is a valuable entropy source for secret key generation (SKG).

A. Secret key generation

SKG builds on three principles: (i) channel reciprocity between Alice and Bob during the channel coherence time, (ii) spatial independence (typically measured through decorrelation), in theory at distances of the same order of magnitude as the wavelength, and (iii) temporal variation, mainly due to node mobility [4]. Spatial decorrelation is particularly important since an eavesdropper (Eve) close to the legitimate users can distil highly correlated sequences and thus substantially decrease the effective size of the key space. Based on Jakes' model, the channel will be uncorrelated when a third party is located half-wavelength away [7]. However, experimental results show that a half-wavelength distance spatial decorrelation is valid only in very rich scattering environments [9]–[12].

Note that in most works, SKG is performed without systematically removing the predictable and spatially or temporally correlated components of the wireless channel coefficients [13]–[15]. To truly achieve spatial decorrelation, the predictable components of the channel state information (CSI) must be disentangled and removed from the remaining components. Furthermore, channel realizations may exhibit non-linear dependencies or the underlying distributions might not be Gaussian; in these cases, correlation is a poor measure of independence. Therefore, there is also a need to extend our investigation to spatial independence as opposed to just spatial decorrelation. To the best of our knowledge, this is the first paper in the literature discussing the importance of spatial independence between legitimate users and potential eavesdroppers at multiple possible locations in the space considered.

B. Localization based node authentication

Authentication requires a predictable and verifiable source of uniqueness, dependent, for example, on the node locations. In other words, the channel components used for authentication must be different for each location though not necessarily decorrelated. Also, it is beneficial if the components do not vary with time [16]. In [17]–[19] physical layer authentication approaches are proposed by exploiting different types of channel parameters. In an earlier contribution, we have shown

1. Muralikrishnan Srinivasan is with Electrical Engineering, Chalmers University of Chalmers University of Technology. (Email:mursri@chalmers.se)

2. Sotiris Skaperas, Mahdi Shakiba Herfeh, and Arsenia Chorti are with ETIS UMR8051, CY University, ENSEA, CNRS, Cergy, France. (Email:sotiris.skaperas, mahdi.shakiba-herfeh, arsenia.chorti@ensea.fr)

M. Srinivisan, S. Skaperas and A. Chorti were supported by CYU INEX funding projects PHEBE and eNiGMA. Also, A. Chorti and M.S. Herfeh were supported by the ELIOT ANR-18-CE40-0030 and FAPESP 2018/12579-7 project.

978-1-5386-8347-7/22/$31.00 ©2022 IEEE

that the first two or three principal components of a principal component analysis (PCA) suffice to largely capture most of the predictable part of the CSI [20].

C. Contributions

Despite the immense bibliography in RF fingerprinting and SKG, a systematic treatment of the CSI as jointly a source of uniqueness and entropy is missing. To the best of our knowledge, only a few papers such as [21], [22] aim to achieve both device authentication and SKG simultaneously in the context of body area networks. At the same time, the proposed method is not practical in a general scenario.

Therefore, this paper aims to fill this gap and build preprocessing approaches for joint SKG and authentication with a fresh perspective by focusing on removing the correlations and dependencies across user locations. In brief,

1) We disentangle the predictable components from the unpredictable components using PCA and two different unsupervised learning methods based on Autoencoders (AE).
2) We discuss in detail the trade-off between SC at transmitter locations and non-reciprocity between the uplink and downlink components used for SKG.
3) We propose to evaluate spatial independence using the d-variable Hilbert-Schmidt independence criterion (dHSIC) [23].
4) We use the total variation distance (TVD) to study spatial uniqueness (in the form of density distance) in the components used for node-authentication.

By employing these preprocessing schemes, the channel components that are the building blocks for the following two cornerstone security operations can be provided simultaneously: (i) spatially decorrelated and independent, but reciprocal components for SKG[1] and (ii) spatially separable but temporally invariant components for node authentication.

II. System Model

Consider single-antenna legitimate nodes, referred to as Alices and a base station referred to as Bob, over a fading channel. Alices' spatial locations are denoted by $\{\mathbf{x}_n\}_{n=1}^N$ $n = 1, \ldots, N$, where $\{x_n\}_{n=1}^N \in \mathbb{R}^L$ and L denotes the spatial dimensions considered (typically $L = 2$). Let the channel function mapping the spatial locations to the $M \times 1$ CSI vectors $\{\mathbf{h}_n\}_{n=1}^N$ denoted by $\mathcal{H} : \mathbb{R}^L \to \mathbb{C}^M$, where M is the number of snapshots in the time domain. Alice and Bob exchange pilot signals so that their respective observations can be modelled as

$$\mathbf{y}_{nu} = \mathbf{h}_n s + \mathbf{n}_{nu},\ n = 1, \ldots, N,\ u \in \{a, b\}, \qquad (1)$$

where the index a denotes an Alice, b denotes Bob; $\mathbf{n}_{na}$ and $\mathbf{n}_{nb}$ are complex circularly symmetric Gaussian noise variables and the pilot symbols s are chosen from binary phase-shift keying (BPSK) constellation [24]. The channel estimates at Alice and Bob, respectively, are denoted by $\mathbf{h}_{na} = \mathbf{y}_{na}$ and $\mathbf{h}_{nb} = \mathbf{y}_{nb}$ for $n = 1, \ldots, N$. Note that we require high-dimensional CSI from as many distinct transmit locations (Alices) as possible to perform accurate preprocessing at fast rates, which is available in all modern wireless systems [25].

[1]Note that tackling the third principle - temporal variation - is beyond the scope of this work

III. Proposed Preprocessing

We learn the functional mapping that captures the predictable spatially correlated components and the unpredictable spatially decorrelated components of the CSI vectors separately, applying: (i) PCA; and (ii) AE. PCA is a linear approach but straightforward and computationally more efficient than AE. On the other hand, AE can capture non-linear dependencies but is also prone to overfitting due to many parameters.

A. PCA

Let $\boldsymbol{H}_u = [\boldsymbol{h}_{1u}, \cdots, \boldsymbol{h}_{Nu}]$ denote the observed channel. $\boldsymbol{U}$ is the $M \times M$ matrix whose rows are the eigenvectors of the matrix $\text{Cov}(\mathbf{H}_u)$, sorted in decreasing order. In many scenarios, e.g., Rician and generally line of sight settings, the first few PCs correspond to the dominant large-scale fading components and the rest of the PCs correspond to the other residual components and noise. Using the eigenvectors $\widehat{D} \times M$ matrix $\boldsymbol{U}_{1:\widehat{D}}$ corresponding to the first $\widehat{D}$ PCs, we compute the dominant predictable part of the observed channel, as follows,

$$\widehat{\boldsymbol{H}}_u = \boldsymbol{U}_{1:\widehat{D}}^H \boldsymbol{W}_u, \qquad (2)$$

where the $\widehat{D} \times M$ matrix $\boldsymbol{W}_u$ is

$$\boldsymbol{W}_u = \boldsymbol{U}_{1:\widehat{D}} \boldsymbol{H}_u, \qquad (3)$$

and $\widehat{\boldsymbol{H}}_u = \left[\widehat{\boldsymbol{h}}_{1u}, \cdots, \widehat{\boldsymbol{h}}_{Nu}\right]$ for $u \in \{a, b\}$ is a $M \times N$ matrix. Once the dominant (predictable) components are removed, we construct the unpredictable part of the observed channel, denoted as $\tilde{\boldsymbol{H}}_u$, using the eigenvectors corresponding to the $\widehat{D}+1$-th PC to $\widehat{D}+\tilde{D}$-th PC, where $\tilde{\boldsymbol{H}}_u = \left[\tilde{\boldsymbol{h}}_{1u}, \cdots, \tilde{\boldsymbol{h}}_{Nu}\right]$ for $u \in \{a, b\}$.

Note that the components beyond $\widehat{D} + \tilde{D}$ are dominated by and neglected while calculating the residuals. To efficiently disentangle into predictable and unpredictable parts, the pair $\{\widehat{D}, \tilde{D}\}$ has to be chosen such that the residuals are independent with minimal effect on the quality of reconciliation between Alices' and Bob's residuals (i.e., the reciprocity between Alices's and Bob's should not be too compromised). We discuss the trade-off between SC (as a measure of independence) and reconciliation for the proposed method in detail in Section V. We will also elucidate how the $\widehat{D}$ dominant components can be used for authentication.

B. Auto-encoders

AE is a neural network that learns two functions, an encoder that maps the M dimensional input matrix $\boldsymbol{h}_{nu}$ into $\widehat{D}$ dimensional encoded values $\boldsymbol{w}_{nu}$ $\forall\ n = 1, \ldots, N$ and for $u \in \{a, b\}$ and a decoder that maps the encoded values back

to an M dimensional output $\widehat{\boldsymbol{h}}_{nu}$, $\forall\ n = 1,\ldots,N$ and for $u \in \{a,b\}$, such that the loss-function

$$E_1 = \frac{1}{N}\sum_{n=1}^{N} \|\boldsymbol{h}_{nu} - \widehat{\boldsymbol{h}}_{nu}\|_2^2, \text{ for } u \in \{a,b\}, \tag{4}$$

which is the mean square error (MSE) is minimal. AE is assumed to implement a denoised $\tilde{D}$-dimensional encoded representation $\boldsymbol{w}_{nu}$, $\forall\ n = 1,\ldots,N$ that can completely encode the dominant components. We treat the output of the decoder $\widehat{\boldsymbol{h}}_{nu}, \forall n = 1,\ldots,N,$ for $u \in \{a,b\}$ as the dominant predictable components under the conjecture that most of the received signal strength is due to large scale fading effects. Here again, we assume that the residuals

$$\left\{\tilde{\boldsymbol{h}}_{nu}(\widehat{D})\right\}_{n=1}^{N} = \{\boldsymbol{h}_{nu} - \widehat{\boldsymbol{h}}_{nu}\}_{n=1}^{N}, \text{ for } u \in \{a,b\} \tag{5}$$

are the unpredictable components of the channel vectors. Also, the value of $\tilde{D}$ is a hyperparameter that must be tuned to balance the desired SC with the reciprocity of the residuals in the uplink and the downlink. Since we want to lower correlation, the loss function can also explicitly specify a correlation term instead of the MSE. In such a case, the following loss function is proposed:

$$E_2 = \frac{1}{N}\sum_{\substack{n_1=1 \\ n_2 \in \mathcal{U}(n_1)}}^{N} \tilde{\boldsymbol{h}}_{n_1u}^H \tilde{\boldsymbol{h}}_{n_2u}, \qquad \text{for } u \in \{a,b\}, \tag{6}$$

as the inner product of the residual at each location and that from the neighbouring locations. Here, $\mathcal{U}(n_1)$ is the nearest neighbours of the n_1-th Alice-Bob pair.

IV. Evaluation of Preprocessing

In this section, we describe the metrics used to evaluate the residuals obtained from the proposed preprocessing and analyze their trade-off for different values of the pair $\{\widehat{D}, \tilde{D}\}$.

A. Spatial decorrelation and independence

The straightforward metric to measure the degree of SC of the residuals between locations is the Pearson correlation coefficient (CC). Given a pair of residuals $\tilde{\boldsymbol{h}}_{n_1u}$ and $\tilde{\boldsymbol{h}}_{n_2u}$ at two locations n_1 and n_2 respectively, the CC is, $\frac{\mathbb{E}\left(\tilde{\boldsymbol{h}}_{n_1u} - \mathbb{E}\left(\tilde{\boldsymbol{h}}_{n_1u}\right)\right)\mathbb{E}\left(\tilde{\boldsymbol{h}}_{n_2u} - \mathbb{E}\left(\tilde{\boldsymbol{h}}_{n_2u}\right)\right)}{\sigma_{\tilde{\boldsymbol{h}}_{n_1u}}\sigma_{\tilde{\boldsymbol{h}}_{n_2u}}}$, where $\sigma_{\tilde{\boldsymbol{h}}_{n_1u}}$ and $\sigma_{\tilde{\boldsymbol{h}}_{n_2u}}$ are the respective standard deviations.

We also explore a kernel-based statistical test of independence abbreviated as $dHSIC$ to determine if the multivariate random variables (RV) are mutually independent [23]. The test applies a positive-definite kernel on the M-dimensional RV and maps its distribution into the reproducing kernel Hilbert space. More precisely, let $\tilde{\boldsymbol{H}} = \left(\tilde{\boldsymbol{h}}_1, \cdots, \tilde{\boldsymbol{h}}_N\right)$ be an $M \times N$ matrix based on the observations of the M-dimensional residuals $\tilde{\boldsymbol{h}}_i = [\tilde{h}_i^1, \cdots, \tilde{h}_i^M]^T$ for $i \in \{1,\cdots,N\}$. The null hypothesis indicates that the $\tilde{\boldsymbol{h}}^j$ for $j \in \{1,\cdots,M\}$ are mutually independent, $H_0 : F_{\tilde{\boldsymbol{h}}^1,\cdots,\tilde{\boldsymbol{h}}^M} = F_{\tilde{\boldsymbol{h}}^1}\cdots F_{\tilde{\boldsymbol{h}}^M}$, whereas the alternative, $H_A : \bar{H}_0$ (not H_0), denotes that $\tilde{\boldsymbol{H}}$ consists of at least two dependent vectors. An estimator $dHSIC_M$ of the statistical functional is as follows [23, Def 2.6],

$$dHSIC_N(\tilde{\boldsymbol{H}}) = \frac{1}{N^2}\sum_{i,j=1}^{N}\prod_{l=1}^{M}\left(\mathbf{1}_{N\times N} \circ K_{ij}^l\right) + \frac{1}{N^{2M}}\prod_{l=1}^{M}\sum_{i,j=1}^{N} K_{ij}^l - \frac{2}{N^{M+1}}\sum_{i,j=1}^{N}\prod_{l=1}^{M}\left(\mathbf{1}_{N\times 1} \circ K_{ij}^l\right), \tag{7}$$

where the operator $\circ$ denotes the Hadamard product and $\mathbf{1}_{N\times N}$ is an $N \times N$ matrix of ones. Also, $\mathbf{K}^l = \left(\mathbf{K}_{ij}^l\right) = \left(k^l(x_i, x_j)\right) \in \mathbb{R}^{N\times N}$ is the Gram matrix of the positive semi-definite Gaussian kernel k^l, defined $\forall x_i, x_j \in \mathbb{R}$ by, $k^l = \exp\left(-\frac{\|x_i - x_j\|^2}{\sigma^2}\right)$, with bandwidth $\sigma = \sqrt{\frac{\text{med}\left(\|x_i - x_j\|^2\right)}{2}}$, where med(.) is the median heuristic.

According to [23, Theorem 3.1], with respect to the hypothesis test at hand, the critical value (for a specific significance level α) can be obtained as below,

$$CV_\alpha = \left[\mathbf{D}^{HSIC}\right]_{\lceil (B+1)(1-\alpha)\rceil + \sum_{i=1}^{B}\mathbb{1}_{\{dHSIC(\tilde{\boldsymbol{H}}) = dHSIC(\tilde{\boldsymbol{H}}_i)\}}},$$

where vector $\mathbf{D}^{HSIC}$ contains the B Monte-Carlo realisations of $dHSIC(\tilde{\boldsymbol{H}})$ in an increasing order; the re-sampling function $dHSIC\left(\tilde{\boldsymbol{H}}\right)$, $\tilde{\boldsymbol{H}} = \left(r_1(\tilde{\boldsymbol{h}}_1), \cdots, r_N(\tilde{\boldsymbol{h}}_N)\right)$ is constructed by $r_1, \cdots, r_N$ random re-samplings without replacement. The operators $\lceil . \rceil$ and $\lfloor . \rfloor_j$ denote the ceiling function and the j-th element of a vector respectively, and $\mathbb{1}_{\{.\}}$ is the indicator function.

Based on the $dHSIC$ procedure, we propose here a normalized-metric,

$$\overline{dHSIC} = \frac{dHSIC(\tilde{\boldsymbol{H}}) - CV_\alpha}{dHSIC(\tilde{\boldsymbol{H}})}\mathbb{1}_{\{dHSIC(\tilde{\boldsymbol{H}}) > CV_\alpha\}}. \tag{8}$$

The $\overline{dHSIC}$ is zero at independence and near zero in case of a low dependence between the variables.

B. Reciprocity and mismatch probability

We use a one-bit quantizer about the median point along the time dimension to check the reciprocity of the residuals in the uplink (Alice to bob) and the downlink (Bob to Alice). The mismatch probability (MP) between Alice and Bob is given by the ratio of the number of bits in error between them to the total number of bits. The quality of reciprocity in both directions is again governed by the parameters $(\widehat{D}, \tilde{D})$ for PCA and the hyperparameter $\widehat{D}$ for AE. Note that the mismatching can be corrected during the information reconciliation stage; however, the higher the MP, the lower the rate of the reconciliation decoder.

C. Total variation distance for authentication

Recall that the output $\widehat{\boldsymbol{h}}_{nu}, \forall n = 1...N,$ for $u \in \{a,b\}$ of the inverse-PCA or the decoder of AE are termed the dominant predictable components of the channel. They depend on the number of dominant PCs $\widehat{D}$ that were discarded after the PCA or the number of neurons in the encoding layer $\widehat{D}$ in the AE.

Note that for an efficient node-authentication, the predictable components between adjacent neighbours must be distinguishable from one another. To measure the separability of the predictable components between neighbouring locations, we use the popular total variation distance (TVD), which measures the distance between the probability density function (PDF) of the sequences. For two probability measures P and Q on a set $\mathcal{X}$, the TVD $d(P,Q)$ is defined as follows

$$d(P,Q) = \frac{1}{2}\sum_{x\in\mathcal{X}} \left|P(x) - Q(x)\right|. \tag{9}$$

As the TVD between two sequences of predictable components increases, the components are more distinguishable and vice-versa. In the next section, we discuss the evolution of TVD for various values of $\widehat{D}$.

V. Numerical Results

To perform simulations, we obtain the channel frequency response (CFR) between transmitters (Alices) at $N = 400$ equi-distant $(1\ m)$ spatial locations within a square area on the ground, between $x = 100$ and $x = 290$ and $y = -100$ and $y = 90$ and a receiver (Bob) at the location $(x, y, z) = (0, 0, 10)$. The number of snapshots are $M = 128$, obtained at a carrier frequency of 2.68 GHz, using the popular Quadriga channel models [26]. To create a temporal variations in the channel, the Alices are assumed to move at a speed of $0.5\ m/s$ and we capture 100 snapshots per second.

A. PCA

First, we study the effect of preprocessing using PCA on the residuals, for SNR $= 20$ dB, in Fig. 1. Figures 1 (a), (b), and (c) illustrate the variation of the three metrics i) average CC between the locations and their nearest neighbours ii) the $\overline{dHSIC}$ iii) the average MP between the Alices and Bob, respectively, with respect to the variation in the pair $\{\widehat{D}, \tilde{D}\}$ in steps of 2. The grid corresponding to $\widehat{D} = 0$ and $\tilde{D} = 0$ indicates no preprocessing. With no preprocessing, the average CC is approximately 0.49, and the MP nearly 0. However, with a sufficient number of dimensions $\tilde{D}$ retained, say $\tilde{D} > 2$, an increase in the number of dimensions omitted $\widehat{D}$ results in a decrease in the CC. Specifically, for $\widehat{D} = 2$ and $\tilde{D} = 20$, we observe a drop in the CC to 0.35, with no significant increase in MP. This is the regime in which the predominant large scale predictable components are removed, and the small scale components are retained. Also, the reciprocity is nearly intact, reflected by the very low MP. This regime is indicated as "Dominance of uncorrelated components" in Fig. 1(a). The corresponding region is referred to as "Low Mismatch Probability" in Fig. 1(c).

Note that, the drop in CC is more pronounced beyond $\widehat{D} = 14$, beyond which most of the predictable components are removed, and the noise becomes dominant. In this regime, the MP also increases due to the impact of noise. This regime is referred to as "Dominance of Noise" in Fig. 1(a). The corresponding region is marked as "High Mismatch Probability" in Fig. 1(c). Note that for $\widehat{D} > 0$ and $\tilde{D} = 2$, the CC of the residuals is large (≈ 1) compared to the original signal. In this regime, the residuals are only two components, which are largely predictable and hence have high CC.

A trend similar to CC, is observed in the average $\overline{dHSIC}$ values in Fig 1(b), especially for higher values of the pair $\{\widehat{D}, \tilde{D}\}$ (in the regime "Statistical Independence") indicating likely independence. On the other hand, $\overline{dHSIC}$ does not follow the CC drop for $\widehat{D} = 2$ and $\tilde{D} \geqslant 10$, indicating the limitations of CC metric compared to $\overline{dHSIC}$, e.g., to capture non linear dependence. In Fig. 2, the trade-offs between CC and MP are shown for SNR$= 5$ dB. As expected, with a decrease in SNR, the effect of noise is more pronounced. Therefore, the regime of noise dominance and high MP is seen even at $\widehat{D} = 10$.

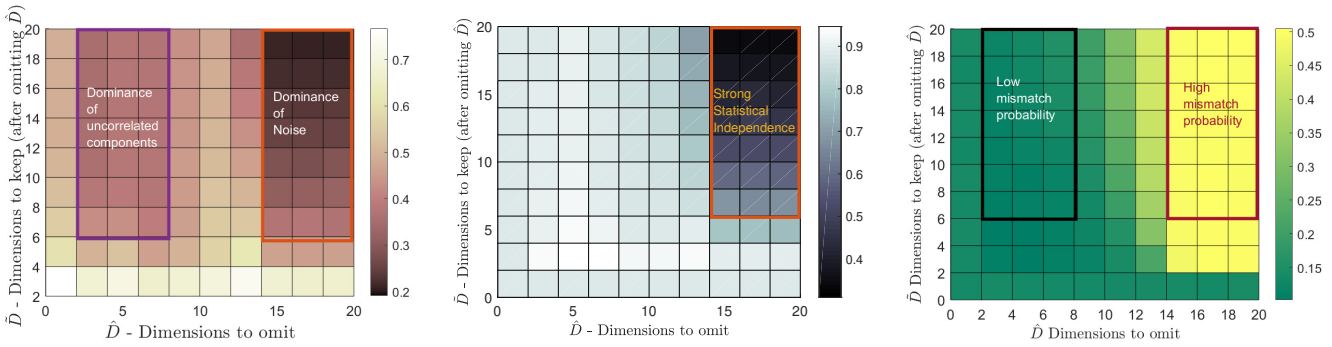
In Fig. 3, the average TVD between the predictable components of Alice and those of her neighbours is plotted for varying $\widehat{D}$. We observe that picking only the first PCA component provides Alice's best separation from her neighbours. The result for $\widehat{D} = 0$ is for the original measurements. With an increase in the SNR, there is a small increase in the TVD. This is because, with an increase in noise, the variance of the predictable components increases and hence TVD decreases. To explain the utility of disentangling the predictable components visually, in Fig. 4, we show the variation of the magnitude of the original channel and the predictable components vs time for six neighbours from the 400 locations. We can observe that when compared to the original signal in Fig. 4(a), the predictable components in Fig. 4(b) are distinguishable and temporally constant.

TABLE I: The layers and activation function for AE1. For AE2 the only change is that the dimensions of the input and the output layers are 400.

Layer	Dimensions	Activation
Input	200	Linear
1	100	tanh
2	50	softplus
3	20	tanh
Intermediate	$\widehat{D}$	linear
4	20	relu
5	50	softplus
6	100	tanh
Output	200	Linear

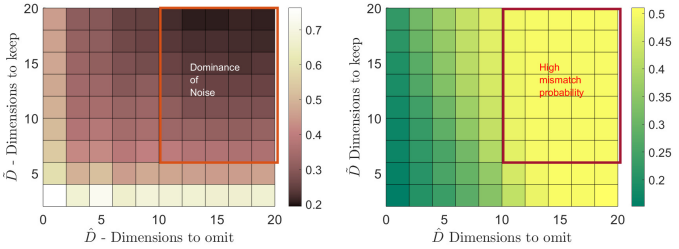
B. AE

The layers and the activation function in the AE are given in Table I and follow the AE in [25]. For brevity, the AE with MSE loss function is referred to as AE1, and that with dot-product loss function is referred to as AE2. The input to the AE2 is formed by grouping the 200×1 CSI vector (100 real and 100 imaginary) of each spatial location with 200×1 long CSI vector from each of the 8 nearest neighbours surrounding the location. In other words, the dimension at the input and the output is 400×1. This ensures that the loss function can minimize the correlation between the users while minimizing the reconstruction error between the input and the output. Two types of training are possible. In localized training, Bob and



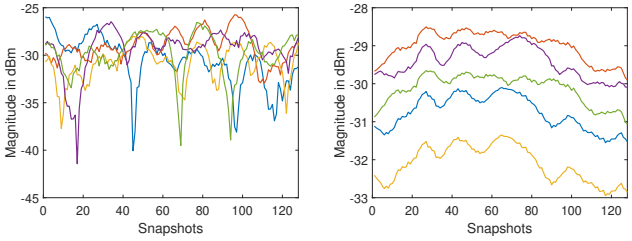
(a) Average CC (b) Average value of the $\overline{dHSIC}$. (c) Average MP

Fig. 1: Trade-off for the Original and Residual components for SNR $= 20$ dB. Darker colours indicate lower values.



(a) Average CC (b) Average MP

Fig. 2: Trade-off for the Original and Residual components for SNR $= 5$ dB



(a) Original signals (b) Predictable components

Fig. 4: Separability of 6 neighbours for the original signal and the predictable component with $\widehat{D} = 1$ for SNR$= 20$ dB

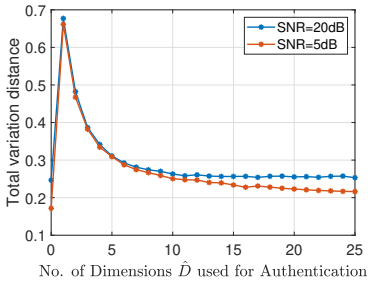


Fig. 3: Total Variation Distance vs $\widehat{D}$

TABLE II: AE: Key results

$\widehat{D}$	1				8			
SNR (dB)	5		20		5		20	
AE type	$AE1$	$AE2$	$AE1$	$AE2$	$AE1$	$AE2$	$AE1$	$AE2$
Original-CC	0.36	0.36	0.48	0.48	0.36	0.36	0.48	0.48
Residual-CC	0.34	0.28	0.44	0.35	0.30	0.20	0.42	0.32
Original-$\overline{dHSIC}$	0.64	0.64	0.82	0.82	0.64	0.64	0.82	0.82
Residual-$\overline{dHSIC}$	0.6	0.58	0.78	0.72	0.43	0.28	0.75	0.75
MP for Localized	0.37	0.39	0.19	0.27	0.39	0.45	0.17	0.36
MP for Centralized	0.35	0.35	0.08	0.08	0.34	0.40	0.10	0.11
TVD Original	0.17	0.17	0.25	0.25	0.17	0.17	0.25	0.25
TVD Predictable	0.19	0.38	0.20	0.42	0.15	0.35	0.18	0.36

the set of Alices train separate AEs with their local data sets. In centralized training, Bob trains an AE with its set of the received signal and distributes the values to the Alices.

From Table II, note that, as in the case of PCA, the lower the SNR, the lower the CC and the higher the MP. Moreover, with an increase in the encoding dimensions $\widehat{D}$, the AE has more freedom to represent the predictable components. Therefore, with an increase in $\widehat{D}$, we observe a drop in the CC. AE2 achieves a CC of 0.32 for $\widehat{D} = 8$ and SNR$= 20$ dB for the residual components, without a significant increase in MP for Centralized training. This CC is lower than what PCA achieves for $\widehat{D} = 2$ and $\tilde{D} = 20$. However, the $\overline{dHSIC}$ of the residuals does not show a significant decrease from that of the original components, especially for SNR$= 20$ dB. This indicates that an independence criterion has to be incorporated in the AE loss function directly, which at present is left for future work. We note in passing that alternatively, dependencies between the residuals can be removed at the final privacy amplification stage of the SKG.

Observe that, in AE2, since the loss function is the dot product between residuals instead of the MSE, we can observe a significant drop in both CC and $\overline{dHSIC}$ of the residuals for AE2 compared to AE1. However, this is accompanied by an increase in the MP, especially in the case of localized training. Also, as expected, centralized training results in a much lower mismatch probability when compared to localized training.

For the case of node-authentication using the predictable components, note that AE1 minimizes the MSE between the original and the predictable components. The AE only attempts to fit the output similar to the original input components in

such a case. Therefore, the TVD remains constant or sometimes even reduces for the predictable components compared to the original components. On the contrary, in AE2, since the loss function is not MSE but the inner product between the residuals, there is no obligation to match the output of the decoder with the input. Hence, the TVD increases in the predictable components.[2] However, an overall observation is that for node authentication, retaining the first PC could be the prefered approach.

As a final point in this discussion, despite the significant MP in some cases, Alice and Bob can reconcile their sequences by using more powerful reconciliation codes. For instance, in one-shot communication between Alice and Bob, Alice sends helper data to Bob through the public channel. Bob corrects the bits in mismatch, utilizing his own generated sequence and the helper message. For example, for $SNR = 20dB$, $\widehat{D} = 2$ and $\tilde{D} = 20$, we can utilize CRC-aided polar codes with list size of 32, to correct all the bits in errors with a coding rate $R = 0.2$ [27]. Finally, we also note that it is possible to explore the working of a dual architecture; PCA can extract the dominant component for authentication, and AE can extract the residuals for SKG.

VI. Conclusions

In this paper, we built and evaluated PCA and AE based preprocessing approaches for disentangling the predictable components from the unpredictable components of wireless fading channel realizations. We discussed in detail the trade-off between SC at transmitter locations and reciprocity or the lack of mismatch between the uplink and downlink for the unpredictable components used for SKG. We also addressed the necessity for a much more decisive spatial independence criterion using dHSIC. We showed, by simulations, the superiority of AE in reducing the SC by incorporating the CC explicitly as a loss function. Finally, we studied the spatial uniqueness in the predictable components used for node-authentication using TVD.

References

[1] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proc. IEEE*, vol. 104, no. 9, pp. 1727–1765, 2016.

[2] V. Mavroeidis, K. Vishi, M. D. Zych, and A. Jøsang, "The impact of quantum computing on present cryptography," *Int. J. of Adv. Comput. Sci. Appl.*, vol. 9, no. 3, pp. 405–414, 2018.

[3] L. Chen, L. Chen, S. Jordan, Y.-K. Liu, D. Moody, R. Peralta, R. Perlner, and D. Smith-Tone, *Report on post-quantum cryptography*. US Department of Commerce, National Institute of Standards and Technology, 2016, vol. 12.

[4] J. Zhang, G. Li, A. Marshall, A. Hu, and L. Hanzo, "A new frontier for iot security emerging from three decades of key generation relying on wireless channels," *IEEE Access*, vol. 8, pp. 138 406–138 446, 2020.

[5] A. Chorti, C. Hollanti, J.-C. Belfiore, and H. V. Poor, "Physical layer security: a paradigm shift in data confidentiality," in *Physical and data-link security techniques for future communication systems*. Springer, 2016, pp. 1–15.

[6] M. Mitev, A. Chorti, M. Reed, and L. Musavian, "Authenticated secret key generation in delay-constrained wireless systems," *EURASIP J. Wirel. Commun. Netw.*, vol. 2020, pp. 1–29, 2020.

[2]Except for MP, the values of CC, $\overline{dHSIC}$ and TVD do not change with the type of training.

[7] A. Goldsmith, *Wireless communications*. Cambridge university press, 2005.

[8] M. Mitev, M. Shekiba-Herfeh, A. Chorti, and M. Reed, "Multi-factor physical layer security authentication in short blocklength communication," *arXiv preprint arXiv:2010.14457*, 2020.

[9] M. Edman, A. Kiayias, Q. Tang, and B. Yener, "On the security of key extraction from measuring physical quantities," *IEEE Trans. Inf. Forensics Sec*, vol. 11, no. 8, pp. 1796–1806, 2016.

[10] C. Zenger, H. Vogt, J. Zimmer, A. Sezgin, and C. Paar, "The passive eavesdropper affects my channel: Secret-key rates under real-world conditions," in *2016 IEEE Globecom Workshops*. IEEE, 2016, pp. 1–6.

[11] R. Dautov and G. R. Tsouri, "Effects of passive negative correlation attack on sensors utilizing physical key extraction in indoor wireless body area networks," *IEEE Sens. Lett.*, vol. 3, no. 7, pp. 1–4, 2019.

[12] Z. Ji, Y. Zhang, Z. He, K. Lin, B. Li, P. L. Yeoh, and H. Yin, "Vulnerabilities of physical layer secret key generation against environment reconstruction based attacks," *IEEE Wireless Commun. Lett.*, vol. 9, no. 5, pp. 693–697, 2020.

[13] G. Li, A. Hu, J. Zhang, L. Peng, C. Sun, and D. Cao, "High-agreement uncorrelated secret key generation based on principal component analysis preprocessing," *IEEE Trans. Commun.*, vol. 66, no. 7, pp. 3022–3034, 2018.

[14] Y. Peng, P. Wang, W. Xiang, and Y. Li, "Secret key generation based on estimated channel state information for tdd-ofdm systems over fading channels," *IEEE Trans. Wireless Commun.*, vol. 16, no. 8, pp. 5176–5186, 2017.

[15] W. Xi, C. Qian, J. Han, K. Zhao, S. Zhong, X.-Y. Li, and J. Zhao, "Instant and robust authentication and key agreement among mobile devices," in *Proc. 2016 ACM SIGSAC Conf. Comput. Commun. Secur.*, 2016, pp. 616–627.

[16] M. Shakiba-Herfeh, A. Chorti, and H. Vincent Poor, *Physical Layer Security: Authentication, Integrity, and Confidentiality*. Springer International Publishing, 2021, pp. 129–150.

[17] X. Wang, P. Hao, and L. Hanzo, "Physical-layer authentication for wireless security enhancement: current challenges and future developments," *IEEE Commun. Mag.*, vol. 54, no. 6, pp. 152–158, 2016.

[18] Q. Li, H. Fan, W. Sun, J. Li, L. Chen, and Z. Liu, "Fingerprints in the air: Unique identification of wireless devices using rf rss fingerprints," *IEEE Sensors J.*, vol. 17, no. 11, pp. 3568–3579, 2017.

[19] H. Fang, X. Wang, and L. Hanzo, "Learning-aided physical layer authentication as an intelligent process," *IEEE Trans. Commun.*, vol. 67, no. 3, pp. 2260–2273, 2018.

[20] M. Srinivasan, S. Skaperas, and A. Chorti, "On the use of csi for the generation of rf fingerprints and secret keys," *To appear in 25th Int. ITG Workshop on Smart Ant.*, 2021.

[21] L. Shi, J. Yuan, S. Yu, and M. Li, "Ask-ban: Authenticated secret key extraction utilizing channel characteristics for body area networks," in *Proc. of the 6th ACM Conf. Secur. Priv. Wireless Mobile Netw.*, 2013, pp. 155–166.

[22] L. Shi, J. Yuan, S. Yu, and M. Li, "Mask-ban: Movement-aided authenticated secret key extraction utilizing channel characteristics in body area networks," *IEEE Internet Things J.*, vol. 2, no. 1, pp. 52–62, 2015.

[23] N. Pfister, B. Buhlmann, and J. P. Scholkopf, "Kernel-based tests for joint independence," *J. R. Stat. Soc. Series B Stat. Methodol.*, vol. 80, no. 1, pp. 5–31, 2018.

[24] A. Chorti, "Optimal signalling strategies and power allocation for wireless secret key generation systems in the presence of a jammer," in *2017 IEEE International Conference on Communications (ICC)*. IEEE, 2017, pp. 1–6.

[25] C. Studer, S. Medjkouh, E. Gonultas, T. Goldstein, and O. Tirkkonen, "Channel charting: Locating users within the radio environment using channel state information," *IEEE Access*, vol. 6, pp. 47 682–47 698, 2018.

[26] S. Jaeckel, L. Raschkowski, K. Börner, and L. Thiele, "Quadriga: A 3-d multi-cell channel model with time evolution for enabling virtual field trials," *IEEE Trans. Antennas Propag.*, vol. 62, no. 6, pp. 3242–3256, 2014.

[27] M. Shakiba-Herfeh and A. Chorti, "Comparison of short blocklength slepian-wolf coding for key reconciliation," in *IEEE Stat. Signal Process. Workshop SSP 2021*, 2021.