Channel State information as a Source of Shared randomness and an Authentication Factor

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).**

Dans cet article, nous concevons des schémas de prétraitement pour dissocier les informations d'état de canal (CSI) en composantes prévisibles et imprévisibles afin de fournir simultanément deux opérations de sécurité clés. Les composantes prévisibles sont utilisées pour l'authentification des nœuds et les composantes imprévisibles pour la génération de clés secrètes (SKG). Pour le cas de la SKG, afin d'empêcher Eve d'exploiter les corrélations spatiales, fréquentielles ou temporelles potentielles avec les utilisateurs légitimes, ce qui réduirait l'espace de clé efficace grâce à une diminution de la taille de l'attaque par force brute, dans ce article, nous mettons l'accent sur la nécessité de réduire la corrélation spatiale (SC) à différents emplacements de transmission. Nous étudions également le compromis entre la SC et la réconciliation en liaison montante et en liaison descendante. De plus, nous discutons de l'importance d'un critère plus robuste - l'indépendance - par rapport à la décorrélation entre les utilisateurs légitimes et les espions. Enfin, nous proposons une métrique pour quantifier l'unicité dans les composantes prévisibles pour l'authentification des nœuds, en utilisant la distance de variation totale (TVD).

I. Introduction

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) [1]–[4].

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) [5]. 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 [6], 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 [1]. Note that in most works, SKG is performed without systematically removing the predictable and spatially or temporally correlated components of the wireless channel coefficients [7]–[9]. 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.

B. Localization based node authentication

Authentication requires a predictable and verifiable source of uniqueness, dependent, for example, on the node locations [10]. 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 [11]. In [12]–[14] physical layer authentication approaches are proposed by exploiting different types of channel parameters. In an earlier contribution, we have shown 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 [15].

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. Arsenia Chorti is also a Wireless Connectivity Research Group Leader at Barkhausen Institut gGmbH, Dresden DE. (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.

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 [16], [17] aim to achieve both device authentication and SKG simultaneously in the context of body area networks. 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) [18].
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

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

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 [19]. 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 [20].

[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,

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

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

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

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).

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:

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

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. 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 [21]. 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

In this study, we investigate the effect of preprocessing using PCA on the residuals for an SNR of 20 dB. Fig. 1 shows the variation of three metrics: i) the average correlation coefficient (CC) between locations and their nearest neighbors, ii) the statistical independence represented by $\overline{dHSIC}$ [18], and iii) the average mismatch probability (MP) between Alices and Bob as a function of the pair $\widehat{D}, \tilde{D}$ in increments of 2. The average correlation coefficient (CC), statistical independence, and average mismatch probability (MP) are examined. With no preprocessing, CC is around 0.49, and MP is nearly 0. For $\widehat{D} = 2$ and $\tilde{D} = 20$, the CC drops to 0.35, with no significant increase in MP. This is the "Dominance of uncorrelated components" regime. Beyond $\widehat{D} = 14$, where most of the predictable components are removed and noise becomes dominant, the drop in CC is more pronounced, and MP increases. This is the "Dominance of Noise" regime. The average $\overline{dHSIC}$ values follow a trend similar to CC, indicating likely independence. However, $\overline{dHSIC}$ does not follow the CC drop for $\widehat{D} = 2$ and $\tilde{D} \geqslant 10$.

In Fig. 2, 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. To explain the utility of disentangling the predictable components visually, in Fig. 3, we show the variation of the magnitude of the original channel and the predictable components vs time for six neighbours from the 400 locations.

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

TABLE II: AE: Key results

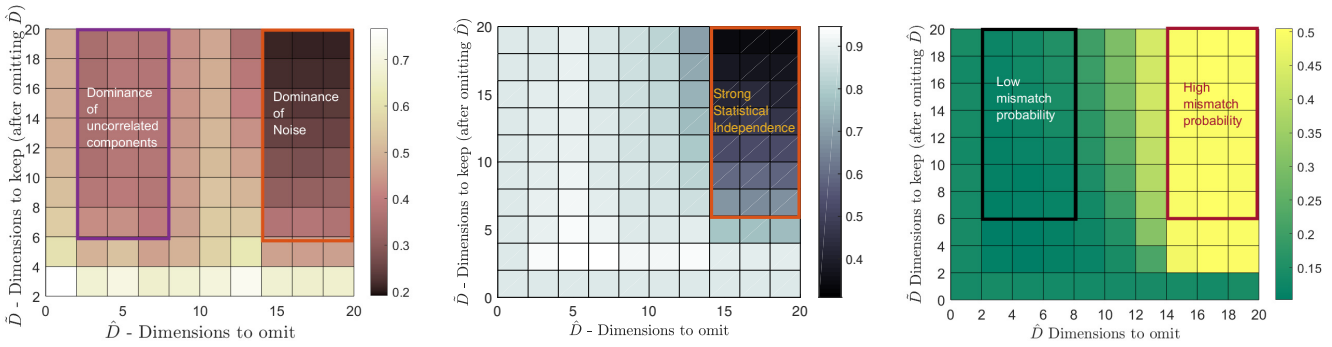
$\widehat{D}$	1				8			
SNR (dB)	5		20		5		20	
AE type	$AE1$	$AE2$	$AE1$	$AE2$	$AE1$	$AE2$	$AE1$	$AE2$
Original-CC	0.36	0.36	0.48	0.48	0.36	0.36	0.48	0.48
Residual-CC	0.34	0.28	0.44	0.35	0.30	0.20	0.42	0.32
Original-$\overline{dHSIC}$	0.64	0.64	0.82	0.82	0.64	0.64	0.82	0.82
Residual-$\overline{dHSIC}$	0.6	0.58	0.78	0.72	0.43	0.28	0.75	0.75
MP	0.35	0.35	0.08	0.08	0.34	0.40	0.10	0.11

B. AE

Table I shows the layers and activation function of the Autoencoder (AE), and it is based on the AE in [20]. There are two types of AE: AE1 with mean squared error (MSE) loss function and AE2 with dot-product loss function. Results for both types of AE are presented in Table II. As shown in Table II, the CC decreases as the SNR decreases and the MP increases. The AE has more freedom to represent predictable components with an increase in encoding dimensions $\widehat{D}$. For AE2, the residual component has a CC of 0.32 at $\widehat{D} = 8$ and SNR$=$ 20 dB, which is lower than the CC achieved by PCA at $\widehat{D} = 2$ and $\tilde{D} = 20$. Incorporating an independence criterion in the AE loss function directly could improve the performance.

V. 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.



(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.

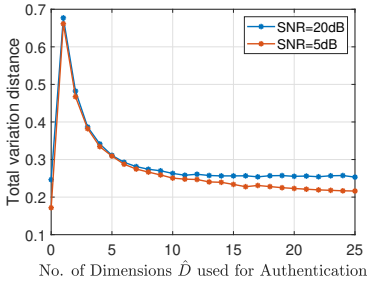
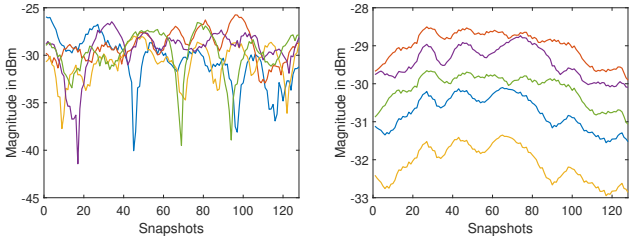


Fig. 2: Total Variation Distance vs $\widehat{D}$



(a) Original signals (b) Predictable components

Fig. 3: Separability of 6 neighbours for the original signal and the predictable component with $\widehat{D} = 1$ for SNR$=$ 20 dB

References

[1] 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.

[2] 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.

[3] 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.

[4] M. Shakiba-Herfeh and A. Chorti, "Comparison of short blocklength slepian-wolf coding for key reconciliation," in *2021 IEEE Statistical Signal Processing Workshop (SSP)*. IEEE, 2021, pp. 111–115.

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

[6] M. Mitev, M. Shakiba-Herfeh, A. Chorti, M. Reed, and S. Baghaee, "A physical layer, zero-round-trip-time, multifactor authentication protocol," *IEEE Access*, vol. 10, pp. 74 555–74 571, 2022.

[7] 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.

[8] 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.

[9] 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.

[10] W. Njima, M. Chafii, A. Chorti, R. M. Shubair, and H. V. Poor, "Indoor localization using data augmentation via selective generative adversarial networks," *IEEE Access*, vol. 9, pp. 98 337–98 347, 2021.

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

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] 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.

[18] N. Pfister, B. Buhlmann, and J. P. Scholkopf, "Kernel-based tests for joint independence," *Journal of the Royal Statistical Society: Series B (Statistical Methodology)*, vol. 80, no. 1, pp. 5–31, 2018.

[19] 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.

[20] 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.

[21] 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.