2023 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom) | 979-8-3503-3782-2/23/$31.00 ©2023 IEEE | DOI: 10.1109/BLACKSEACOM58138.2023.10299798

Carrier Frequency Offset Based Shared Randomness for Secure Transmission in M-PSK NOMA

Caner Göztepe*, Güneş Karabulut Kurt† and Berna Özbek‡
*Dept. of Electronics and Communication Engineering, Istanbul Technical University, Istanbul, Türkiye
†Dept. of Electrical Engineering, Polytechnique Montréal, Montréal, Canada
‡Dept. of Electrical-Electronics Engineering, Izmir Institute of Technology, Izmir, Türkiye
goztepe@itu.edu.tr, gunes.kurt@polymtl.ca, bernaozbek@iyte.edu.tr

***Abstract*—Power domain non-orthogonal multiple access (NOMA) enhances spectral efficiency by superposing multiple users in the same time-frequency resource block at the expense of exposing the users' data. However, current approaches to improve the secrecy levels of users are limited to rate reduction. This paper proposes a secure NOMA system based on the shared randomness extracted from the reciprocal carrier frequency offsets (CFOs) between the transmitter-receiver pairs for M-ary phase-shift keying. As multiple users will have physically separated oscillators, it will result in independent CFOs among users. This randomness is used to introduce a constellation rotation in the transmitted symbols. We show that under ideal CFO estimates, the proposed approach achieves perfect secrecy among all NOMA users without introducing any rate reduction. We also demonstrate the practical applicability of the proposed approach by using a software-defined radio-based test bed.**

***Index Terms*—Carrier frequency offset, non-orthogonal multiple access (NOMA), physical layer security, perfect secrecy, software-defined radio.**

I. Introduction

The power domain non-orthogonal multiple access (NOMA) system embodies the potential to significantly improve the spectral efficiency of wireless systems by using the superposition property at the cost of an increase in the receiver complexity [1]. The users who share the same time-frequency resource block are differentiated based on their distinct power levels and channel gains. NOMA systems are frequently composed of two users: the strong user (i.e., the user with a higher channel gain) and the weak user (i.e., the user with a lower channel gain). However, using the same time-frequency resource block also introduces a security vulnerability among the strong and the weak users since the users can detect each others' symbols without prior authorization.

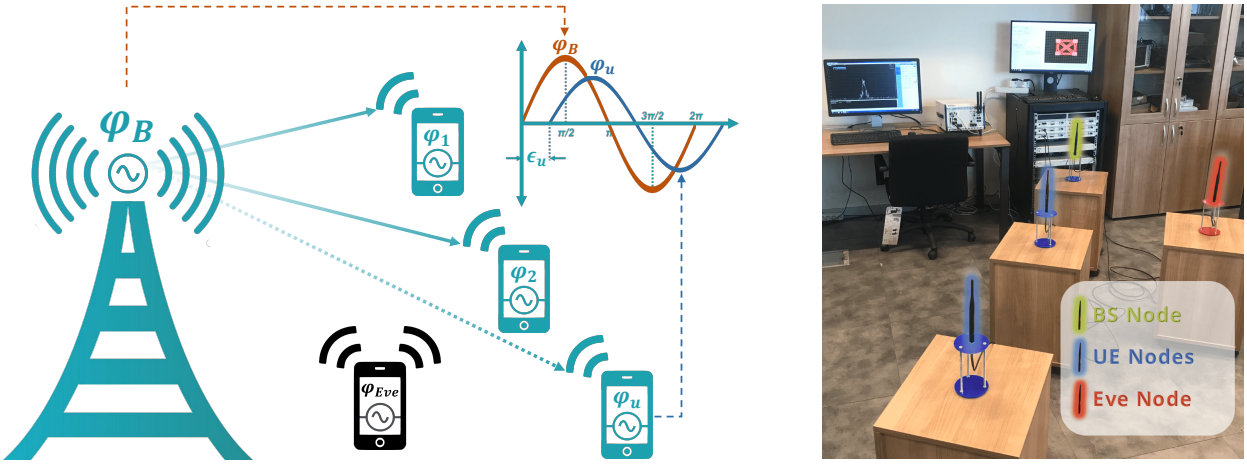
The information that innocuous/malicious listeners can extract at the bit level can be limited by utilizing the physical properties of the wireless communications through physical layer security (PLS). PLS is one of the most prominent research topics, as it does not impose any computational constraints and can operate as a complementary solution for security techniques at the upper layers [2]. In recent years, several studies have been conducted to address the security issue of a NOMA system including the key-based security approaches. In [3], the authors examined the secret key-based schemes that address the NOMA system's privacy and authentication issues by encrypting and decrypting secret messages. However, when the private key security is breached, the confidential information can be easily captured and exposed. Consequently, the keyless PLS schemes are preferred as they do not require any secret keys for encryption/decryption data [4].

As a new perspective on the security of NOMA systems, the authors in [5] use PLS to hide the information symbols by combining a lower symbol alphabet and directional modulation vectors in an optimal manner while investigating the sum rate and the secrecy rate performances. Despite the reduced data rate, a gain is observed in terms of security for only two users through a successive interference cancellation (SIC) decoder by targeting the protection of the weak user against the strong user. Therefore, it cannot be generalized in the presence of a maximum likelihood (ML) estimator in a straightforward manner and the scheme cannot support more than two simultaneous users.

It is essential to realize a secure and less complex system without reducing the data rate in NOMA using PLS. The authors in [6] designed a secure NOMA system compared to traditional methods, especially against internal Eve. They also carried out the power optimization to guarantee the data rate and reached to the targeted secrecy rate. In [7], the phase shifts were introduced in the symbols based on the channel characteristics of each user. However, since the channel characteristic can be learned by an external eavesdropper (*Eve*), the performance of PLS begins to deteriorate.

The authors in [8] have improved the performance of PLS against untrusted near user and Eves by using the joint beamforming and power allocation and joint artificial noise aided beamforming and power allocation. However, the complexity of these schemes are increased with the number of antennas at the BS due to the use of iterations.

Addressing the limitations in the literature, in this paper, we use shared information, extracted from the carrier frequency offsets (CFOs) of the oscillators, between a transmitter and receiver pair. CFO is a parameter that needs to be estimated and compensated in all wireless communication systems [9]. However, obtaining high accuracy levels in CFO estimation often requires a high signal-to-noise ratio (SNR) and faultless hardware infrastructure [10]. The *reciprocal CFO* between the transmitter-receiver pairs has long been investigated in the literature, accompanied by measurement-based evidence [11],



(a) (b)

Figure 1: (a) The proposed scheme for the secure NOMA system. b) The real-time (RT) test bed.

[12]. In line with the above-noted statements, having observed the independence of the CFO estimates between one transmitter (receiver) and multiple receivers (transmitters) clocks, we propose to use this shared information in NOMA systems with M-ary phase-shift keying (M-PSK), as depicted in Fig. 1. This shared randomness has not yet been considered for a secure NOMA transmission to the best of our knowledge. Using this shared randomness from the estimated CFOs, we implement a practically relevant secure NOMA transmission scheme. In the literature, there are limited NOMA test beds [13], [14]. However, a secure NOMA system is not yet reported, and in this paper, we address this gap in the literature. The contributions of this work are detailed below.

Contribution 1: We propose a keyless PLS technique that applies to power domain NOMA systems with M-PSK modulation. Our proposed approach uses a quantized CFO estimate at the base station (BS) and all NOMA users to introduce ambiguity in the transmitted symbols. As the constellations are not distorted and no lower-order constellation is forced, no rate loss is observed.

Contribution 2: We create a test bed to prove that the keyless PLS technique, which we propose theoretically, is applicable in real life. The proposed secure system is quantified in a realistic setting where the CFO estimates are not ideal through extensive measurements.

The rest of this paper is organized as follows. In Section II, the system model is introduced. We propose the secure NOMA system in Section III. The test-bed description is reported in Section IV. Section V contains the simulation and the measurement results. Finally, in Section VI, conclusions are drawn.

II. System Model

This section focuses on the downlink transmission; while, the same approach can easily be extended to the uplink transmission. The BS is serving U users, and all nodes have one antenna. The transmitted symbol to the u^{th} user $(1 \leq u \leq U)$ is denoted by x_u, where $x_u \in \mathcal{S}$ where the symbol set of an M-PSK constellation of $\mathcal{S} = \left\{1, e^{j\frac{2\pi}{M}}, \ldots, e^{j\frac{2\pi(M-1)}{M}}\right\}$. φ_B and φ_u denote the local oscillator frequencies in the BS and the u^{th} user equipment (UE), respectively. Let us define the normalized CFO as ϵ_u between the BS and the u^{th} user, $\epsilon_u \in (-\pi, \pi]$, as a ratio of the CFO to carrier spacing $\Delta\varphi$, given as;

$$\epsilon_u = \frac{\varphi_B - \varphi_u}{\Delta\varphi}. \tag{1}$$

We define the information symbol of the u^{th} user as $s_u \in \mathcal{S}$, and assume that the priori distributions of x_u and s_u are identical. Aiming to introduce shared randomness in the users' symbols, we map the information symbol s_u to the transmitted symbol x_u by using a random rotation extracted from the reciprocal CFO estimates between the u^{th} user and the BS according to;

$$x_u = e^{jQ(\epsilon_u)} s_u, \tag{2}$$

where $Q(\epsilon_u)$ is an M-level uniform quantizer. Hence, the rotation preserves the same constellation for both s_u and x_u.

The transmitted power domain NOMA symbol is given as;

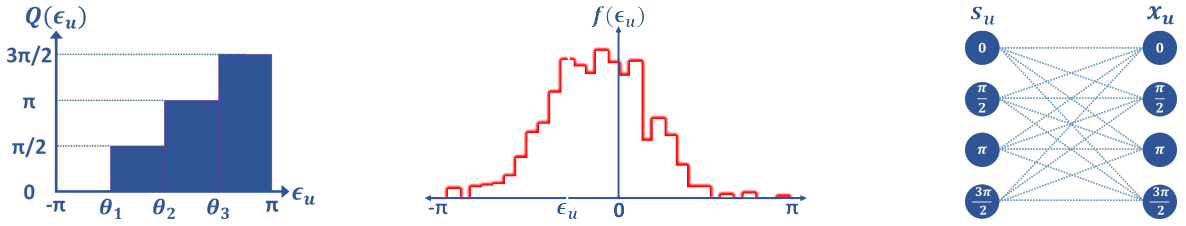
$$x = \sum_{u=1}^{U} \sqrt{\alpha_u}\, x_u = \sum_{u=1}^{U} \sqrt{\alpha_u}\, e^{jQ(\epsilon_u)} s_u, \tag{3}$$

where α_u is the corresponding power coefficient, and $\sum_{u=1}^{U} \alpha_u = 1$.

Then, the received signal at the u^{th} user can be modeled as;

$$r_u = \sqrt{\ell_u} h_u e^{j2\pi\epsilon_u} x + n_u, \tag{4}$$

where ℓ_u is the path loss coefficient inversely proportional to the distance between the u^{th} user and BS, and n_u denotes the additive white Gaussian noise with zero mean and variance σ_u^2. The channel represented by h_u between the base station and the u^{th} user can be modeled as either Rayleigh or Rician distribution. In the considered NOMA scheme, the users are



(a) (b) (c)

Figure 2: (a) Quantization point selection for QPSK. (b) An exemplary probability density function of CFO. (c) Mapping from s_u to x_u for QPSK.

sorted in descending order where the first user is the strongest one and U^{th} user is the weakest one.

The estimation of normalized CFO, $\tilde{\epsilon_u}$, can be obtained by using the ML estimator or Moose method [9]. Then, the received signal at the u^{th} user after the CFO compensation is expressed as;

$$r_u = e^{-j2\pi\tilde{\epsilon}_u}\ e^{-jQ(\tilde{\epsilon}_u)}\ \sqrt{\ell_u}h_u\ e^{j2\pi\epsilon_u}\sum_{u=1}^{U}\sqrt{\alpha_u}\ e^{jQ(\epsilon_u)}s_u + e^{-j2\pi\tilde{\epsilon}_u}\ e^{-jQ(\tilde{\epsilon}_u)}\ n_u. \tag{5}$$

III. Proposed Secure NOMA

The privacy problem of the traditional method becomes apparent in both SIC and ML detectors, as all information of other users can be detected by any user. In the proposed method as in Algorithm 1, (2) introduces shared randomness and as a result, it brings ambiguity to the other users' symbols. Since the CFOs of other users cannot be obtained by the u^{th} user, this user can not detect the information of the other users. This is also valid for malicious Eve, and all user's information can remain confidential for other ones.

Algorithm 1 The Proposed Secure NOMA System

- Transmit pilot frames for CFO estimation from UEs to the BS.
- Quantize the normalized CFO values of each UE at the BS in accordance with (6).
- Generate new symbols, x_u, for each UE considering quantized CFO as in (2).
- Generate a NOMA symbol, x, to be transmitted according to the power allocation coefficients, as in (3).

A. Secrecy Performance Analysis

Firstly, we investigate the security performance under ideal conditions assuming that the CFO estimates are ideal, i.e., $\epsilon_u = \hat{\epsilon}_u$, $\forall u$. The effect of real-life implications on the system performance will be given in the next section. The CFO between the u^{th} user and the l^{th} user are independent due to their physically disjoint oscillator pairs as in Appendix.

Let us denote the random variables that represent s_u by S_u and x_u by X_u. Recall that the information symbols which are represented by S_u are independent and uniformly distributed, i.e. $p(S_u = s_u) = \frac{1}{M}$, where $p(\cdot)$ represents the probability function.

Our aim is to ensure perfect secrecy, i.e. X_u should not reveal any information about S_u. This is ensured if and only if $H(S_u/X_u) = 0$, where $H(\cdot)$ represents the equivocation function (conditional entropy).

Theorem 1. *Assuming that sampled CFO values are independent and identically distributed, it is possible to obtain perfect secrecy, i.e. $H(S_u/X_u) = 0$, for an arbitrary CFO distribution, $f(\epsilon_u)$.*

Proof. Let us denote a quantized CFO sample of the u^{th} user by $z_u = e^{jQ(\epsilon_u)}$, and the corresponding random variable by Z_u. The range set of the M-level quantizer, $Q(\cdot)$, is identical to the selected modulation constellation $\mathcal{S}_u$. For an arbitrary distribution, $f(\Upsilon_u)$, it is possible to design a quantizer such that $P(Z_u = z_u) = \frac{1}{M}$. The algorithmic solutions to this problem are available to determine the quantization boundaries θ_m, including [15], revealing;

$$\int_{-\pi}^{\theta_m} f(\Upsilon_u)\, d\epsilon_u = \frac{m}{M}, \quad \text{where} \quad \begin{matrix} 1 \le m < M \\ -\pi < \theta_m < \pi \end{matrix} \tag{6}$$

and $X_u = Z_u S_u$. In this case,

$$H(S_u/X_u) = \sum_{X_u, S_u \in \mathcal{S}} p(X_u, S_u) \log \frac{\sum_{Z_u \in \mathcal{S}_u} p(X_u, S_u/Z_u) p(Z_u)}{p(X_u)}$$

and for a given X_u, since Z_u is independent from S_u and X_u, and additionally $p(Z_u) = p(X_u) = \frac{1}{M}$, it can be seen that $\sum_{Z_u \in \mathcal{S}} p(X_u, S_u/Z_u) p(Z_u) = p(X_u)$, hence $H(S_u/X_u) = 0$, providing perfect secrecy for S_u. □

The quantization intervals for QPSK in (6) and the conversion of x_u to s_u according to the CFO values are shown in Fig. 2. Here, each modulation symbol of x_u can be mapped to all modulation symbols of s_u with a probability of $\frac{1}{M} = \frac{1}{4}$ for QPSK.

Corollary 1. *The proposed system is a secure power domain NOMA system with no compromise from the transmission rate.*

Proof. From Theorem 1, it is clear that under ideal conditions, the received symbol, r_u does not reveal any information about the transmitted information, X_u. Hence, received symbol r_ℓ for $u \neq \ell$ does not reveal any information about X_u to the ℓ^{th} user, while X_ℓ can be detected since Y_ℓ is available due to the

reciprocity of the ϵ_ℓ. Since only phase rotations are included in the system model, the data rate is kept the same as the traditional NOMA system. □

Corollary 2. *The proposed system provides perfect secrecy against possible Eve.*

Proof. Since S_u is only available at the u^{th} user due to the physically confined placement of local oscillators, without this information any *Eve* cannot detect the transmitted information symbol X_u which can be detected if and only if an exhaustive search is employed. □

Corollaries 1 and 2 ensure the security of the proposed system under the ideal estimation of CFOs at each user. The main concerns in this idealized scenario are the distributions of the CFO values, their reciprocity, and independence. In the following section, these aspects are investigated in detail through measurement results, in line with real deployments.

B. Secrecy Rate Calculation

In the presence of a malicious user which can be either an internal eavesdropper or *Eve*, the average secrecy rate belonging to legitimate user u is determined by;

$$R_u^s = \max\Big\{0, \mathbb{E}[R_u - R_e]\Big\} \tag{7}$$

where R_u is the data rate of legitimate user u and R_e is the data rate of the internal eavesdropper or *Eve*.

For both traditional NOMA and the proposed system, the average secrecy rates are calculated in accordance with [16] by using SIC detection. For the proposed NOMA system with two users, in the presence of either an internal eavesdropper or *Eve*, the secrecy rates are given, respectively;

$$R_1^s = \log_2\left(1 + \frac{\alpha_1|h_1|^2}{\sigma_1^2}\right) \tag{8}$$

$$R_2^s = \log_2\left(1 + \frac{\alpha_2|h_2|^2}{\alpha_1|h_2|^2 + \sigma_2^2}\right) \tag{9}$$

Here, the secrecy rates are determined based on data rates of the legitimate users since $R_e = 0$ for both the internal eavesdropper and *Eve*. For legitimate user 1, the reason is that the $e^{jQ(\epsilon_1)}$ in (5) is only known by user 1 and it is just a random variable for both the *Eve* and the user 2 which acts as an internal eavesdropper. Therefore, s_1 and x_1 becomes independent at user 2 and *Eve* as a result of randomness revealed by the proposed scheme, and x_1 cannot be used to decode s_1 at both user 2 and *Eve*. A similar approach applies where user 2 is the legitimate user. Consequently, maximum secrecy rates can be achieved through the proposed method.

IV. Software-Defined Radio test bed

This section presents the test bed used in real-time (RT) tests. The test system created, as shown in Fig. 1b, consists of 4 nodes on 4 USRP-2943Rs. The LabVIEW programming software on the host computer, which is used for the configuration, control, and data collection aspects of the transmitter and receivers, controls one transmitter node, two UE nodes, and one *Eve* node. There is 1 meter between the transmitter and the first user (UE_1) while UE_1, *Eve* and the second user (UE_2) are positioned in straight order, with a distance of a half meter between two adjacent nodes. The path loss measured per a half meter is approximately 5 dB. The power coefficients ratio is determined as $\frac{\alpha_1}{\alpha_2} = \frac{1}{5}$. The single carrier QPSK modulation method with a root-raised cosine filter of roll-off factor 0.6 is used in the system. Pilot symbols are utilized for CFO estimation, and channel estimation by the least square method in RT tests performed in the 2.45GHz frequency band and 1MHz bandwidth, and the pilot symbol/data symbol rate is determined as 1/4. The pilot symbols are modulated by using BPSK. The pilot symbols are also used for the estimation of SNR. 20M data samples are used for each SNR level.

V. Simulation and Measurement Results

In this section, the performance of the proposed secure NOMA system for two users by CFO-based shared randomness is evaluated both in a simulation and in an RT test environment. In RT tests, since the local oscillators in the devices are different, the cross-correlation of the CFO values of all nodes with the transmitter is measured separately as zero. As a result, it is verified by the tests that four different nodes are statistically independent of each other and theoretically obtained perfect secrecy is also obtained in the RT test environment. In this case, while users can only obtain the correct data about themselves, they can receive random data about other users. The *Eve* can only have random data about each user.

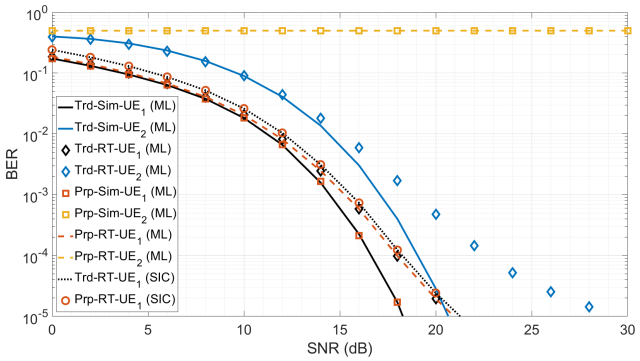


Figure 3: Error performances for the traditional (Trd) and proposed (Prp) methods at the UE_1 in both real-time (RT) and simulation (Sim) environments using ML or SIC detectors.

Considering that the local oscillator of each device is different in terms of hardware, each UE can only have mutual information about its corresponding device. If there is no hardware attack, the nodes in different locations cannot have information about each other's CFO values. However, when the *Eve* node knows the local oscillator frequency perfectly, the security performance of the proposed technique can be increased by using hybrid-key-based PLS. Accordingly, there is no data leakage between the legitimate user and malicious listeners, thanks to the PLS generated by CFO.

We evaluate the Pearson correlation coefficients between all nodes in the RT test environment. Pearson correlation coefficients obtained using CFO values among all nodes, measured between 10^{-9} and 10^{-6}, are approximately equal to 0 which results that the CFO values among all nodes are statistically independent.

The QPSK modulation scheme is used in both simulation and RT test environments. According to the RT tests and (6), the θ_m values are determined as $\theta_1 = -207$Hz, $\theta_2 = 18$Hz, and $\theta_3 = 155$Hz to yield almost equal mapping probabilities.

Rician fading channel with K =10 parameter is used in the simulation following the RT test environment. The error performances of UE_1 are shown in Fig. 3. Unlike the simulation cases, the error floor occurs due to the estimation errors in RT tests. UE_1 has the same error performance when using the traditional or the proposed method. However, through the traditional NOMA, UE_1 can also obtain information about UE_2 due to the NOMA's security problem. In the proposed NOMA, UE_1 has no knowledge about the UE_2, and perfect secrecy is provided.

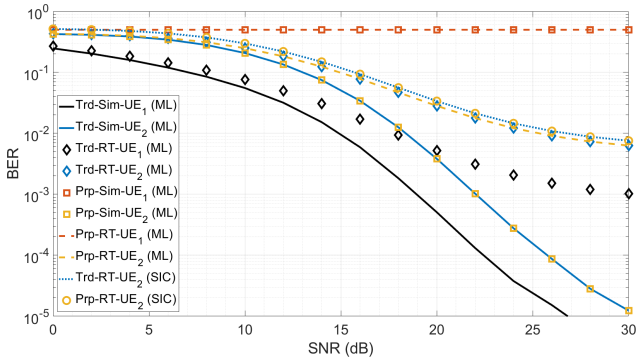


Figure 4: Error performances for the Trd and Prp methods at the UE_2 in both RT and Sim environments using ML or SIC detectors.

Similarly, as shown in Fig. 4, it is seen that there is no difference in terms of the error performance of the UE_2 in both the traditional and the proposed method. The fact that the UE_2 has information about the UE_1 poses a security problem in the traditional NOMA. The proposed method achieves perfect secrecy at the UE_2 in both simulation and RT test environments.

In addition, Fig. 3 and Fig. 4 show that the proposed method is still effective, although there is a decrease in error performance when the SIC detector is used instead of the ML detector. There might also be an *Eve* in the system. The performance of *Eve* in both the traditional and the proposed systems for two-user NOMA are shown in Fig. 5. It is assumed that *Eve* knows the pilot symbols, power allocation coefficients and channel characteristics of all nodes, and uses ML detector. In the traditional two-user NOMA, *Eve* can obtain data for both the UE_1 and the UE_2. Through the proposed two-user NOMA, providing perfect secrecy, *Eve* cannot obtain data about the legitimate user.

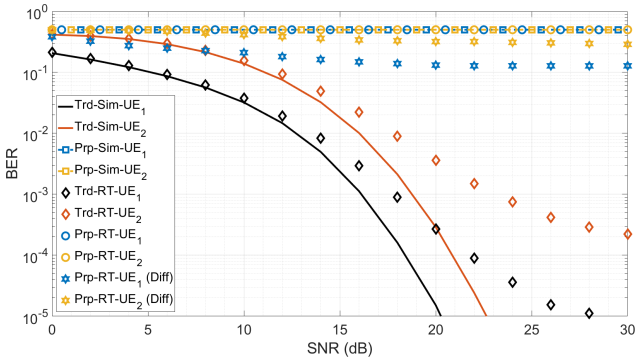


Figure 5: Error performances for the Trd and Prp methods at the *Eve* in both RT and Sim environments using ML detector.

With the help of the signal processing algorithms and faultless hardware infrastructure, *Eve* can only partially estimate the CFO values to decode the legitimate users' data. For instance, *Eve* can estimate the CFO between itself and the users, and between itself and the BS by using pilots. Then, it can calculate the CFO values available at the BS by taking the difference between these estimates. Using this method, the BER obtained by *Eve* in the real-time test environment is shown as a difference case (Diff) in Fig. 5. Only a 13% correlation is determined between the CFO values calculated at the *Eve* and the BER is still high by the result of the proposed method.

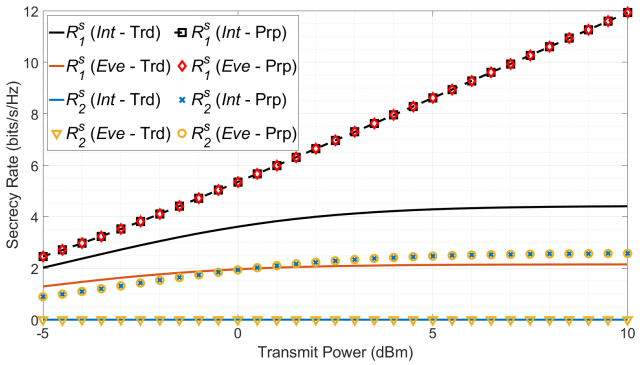


Figure 6: Secrecy rates for both the traditional and the proposed two-user NOMA system in the presence of internal eavesdropper (*Int*) or *Eve*.

In the presence of 5dB path loss between each node, the secrecy rates for the legitimate users are shown in Fig. 6 under ideal conditions. When the traditional NOMA is used, a positive secrecy rate can be obtained for the first user in the presence of an internal eavesdropper or *Eve*. However, for the second user, the secrecy rate becomes zero for both the internal eavesdropper and *Eve* due to its position and the power allocation coefficients. This demonstrates a significant security problem in NOMA. On the other hand, when the proposed method is used, none of the malicious listeners can obtain the data of legitimate users correctly. Thus, the secrecy rate is maximized, regardless of the positioning and power

allocation coefficients.

All the information obtained by two users and *Eve* proves that the proposed method is admittedly successful. Perfect secrecy is achieved without making any profound changes to the traditional method. The proposed method provides an efficient solution to the fundamental security problem of NOMA. Furthermore, the results obtained from the RT tests show that the proposed method is easily applicable.

VI. Conclusion

This article proposed a CFO-based shared randomness method, which provides perfect secrecy for M-PSK modulated NOMA. The performance of the proposed method has been obtained both through simulations and real-time tests conducted using the designed test bed with software-defined radio nodes. For future studies, the proposed approach will be extended to the M-QAM modulation scheme, multi-carrier waveforms and M-PSK with different quantizer resolutions. Moreover, a new hybrid-key-based PLS technique using the proposed technique will be suggested.

Appendix

Let A and B define the sequences of A_j and B_j for $\forall j \in \{1, \ldots, N\}$, respectively. If $\rho(A, B)$, which represents the Pearson correlation coefficient in (10) of the A and B sequences, is equal to zero, these two sequences are statistically independent [17]

$$\rho(A, B) = \frac{1}{N-1} \sum_{j=1}^{N} \left(\frac{A_j - \mu_A}{\sigma_A} \right) \left(\frac{B_j - \mu_B}{\sigma_B} \right), \tag{10}$$

where μ_A and σ_A are the mean and standard deviation of A, respectively. Also, μ_B and σ_B are the mean and standard deviation of B. Let Φ_u and Φ_k define the sequences of CFO values for the user u and the user k, respectively. Due to the physical backgrounds of the receivers, we would expect

$$\rho(\Phi_u, \Phi_k) = 0, \tag{11}$$

for $\forall u, k \in \{1, \ldots, U\}$ and $u \neq k$.

References

[1] M. Aldababsa, M. Toka, S. Gökçeli, G. K. Kurt, and O. Kucur, "A tutorial on nonorthogonal multiple access for 5G and beyond," *Wireless Comm. and Mobile Comp.*, vol. 2018, 2018.

[2] Y. Qi and M. Vaezi, "Signaling design for MIMO-NOMA with different security requirements," *IEEE Transactions on Signal Processing*, vol. 70, pp. 1389–1401, 2022.

[3] N. Xie, Q. Zhang, J. Chen, and H. Tan, "Privacy-preserving physical-layer authentication for non-orthogonal multiple access systems," *IEEE Journal on Selected Areas in Communications*, vol. 40, no. 4, pp. 1371–1385, 2022.

[4] B. Van Nguyen, H. Jung, and K. Kim, "Physical layer security schemes for full-duplex cooperative systems: State of the art and beyond," *IEEE Communications Magazine*, vol. 56, no. 11, pp. 131–137, 2018.

[5] R. M. Christopher and D. K. Borah, "Physical layer security for weak user in MISO NOMA using directional modulation (NOMAD)," *IEEE Communications Letters*, vol. 24, no. 5, pp. 956–960, 2020.

[6] C. Zhang, F. Jia, Z. Zhang, J. Ge, and F. Gong, "Physical layer security designs for 5G NOMA systems with a stronger near-end internal eavesdropper," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 11, pp. 13 005–13 017, 2020.

[7] A. Abushattal, S. Althunibat, M. Qaraqe, and H. Arslan, "A secure downlink NOMA scheme against unknown internal eavesdroppers," *IEEE Wireless Communications Letters*, vol. 10, no. 6, pp. 1281–1285, 2021.

[8] K. Cao, B. Wang, H. Ding, T. Li, J. Tian, and F. Gong, "Secure transmission designs for NOMA systems against internal and external eavesdropping," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 2930–2943, 2020.

[9] F. Ling, *Synchronization in Digital Communication Systems*. Cambridge University Press, 2017.

[10] M. Zhou, Z. Feng, Y. Liu, and X. Huang, "An efficient algorithm and hardware architecture for maximum-likelihood based carrier frequency offset estimation in MIMO systems," *IEEE Access*, vol. 6, pp. 50 105–50 116, 2018.

[11] W. Hou, X. Wang, J.-Y. Chouinard, and A. Refaey, "Physical layer authentication for mobile systems with time-varying carrier frequency offsets," *IEEE Transactions on Communications*, vol. 62, no. 5, pp. 1658–1667, 2014.

[12] W. Aman, A. Ijaz, M. M. U. Rahman, D. N. K. Jayakody, and H. Pervaiz, "Shared secret key generation via carrier frequency offsets," in *2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring)*, 2019, pp. 1–5.

[13] X. Wei, Z. Geng, H. Liu, K. Zheng, and R. Xu, "A portable SDR non-orthogonal multiple access testbed for 5G networks," in *2017 IEEE 85th Vehicular Technology Conference (VTC Spring)*, 2017, pp. 1–5.

[14] C. Goztepe, B. Ozbek, and G. Karabulut Kurt, "Design and implementation of spatial correlation-based clustering for multiuser MISO-NOMA systems," *IEEE Comm. Letters*, vol. 25, no. 1, pp. 254–258, 2020.

[15] R. M. Gray and D. L. Neuhoff, "Quantization," *IEEE Trans. on Info. Theory*, vol. 44, no. 6, pp. 2325–2383, 1998.

[16] W. Yu, A. Chorti, L. Musavian, H. V. Poor, and Q. Ni, "Effective secrecy rate for a downlink NOMA network," *IEEE Transactions on Wireless Communications*, vol. 18, no. 12, pp. 5673–5690, 2019.

[17] J. Benesty, J. Chen, Y. Huang, and I. Cohen, *Noise reduction in speech processing*, ser. Springer Topics in Signal Processing. Springer Berlin Heidelberg, 2009.