Physical Layer Anonymous Precoding:
The Path to Privacy-Preserving Communications

Zhongxiang Wei, *Member, IEEE,* Christos Masouros, *Senior Member, IEEE,* H. Vincent Poor, *Life Fellow, IEEE,*
Athina P. Petropulu, *Fellow, IEEE,* and Lajos Hanzo, *Fellow, IEEE*

Abstract—Next-generation systems aim to increase both the speed and responsiveness of wireless communications, while supporting compelling applications such as edge/cloud computing, remote-Health, vehicle-to-infrastructure communications, etc. As these applications are expected to carry confidential personal data, ensuring user privacy becomes a critical issue. In contrast to traditional security and privacy designs that aim to prevent confidential information from being eavesdropped upon by adversaries, or learned by unauthorized parties, in this paper we consider designs that mask the users identities during communication, hence resulting in anonymous communications. In particular, we examine the recent interest in physical layer (PHY) anonymous solutions. This line of research departs from conventional higher layer anonymous authentication/encryption and routing protocols, and judiciously manipulates the signaling pattern of transmitted signals in order to mask the senders' PHY characteristics. We first discuss the concept of anonymity at the PHY, and illustrate a strategy that is able to unmask the senders identity by analyzing his/her PHY information only, i.e., signalling patterns and the inherent fading characteristics. Subsequently, we overview the emerging area of anonymous precoding to preserve the sender's anonymity, while ensuring high receiver-side signal-to-interference-plus-noise ratio (SINR) for communication. This family of anonymous precoding designs represents a new approach to providing anonymity at the PHY, introducing a new dimension for privacy-preserving techniques.

I. INTRODUCTION

The development of 5G communications has deeply influenced the era of computing, storage and communications. The emerging applications are expected to carry confidential personal data, such as private data offloading in edge computing, real-time monitoring of vital physiological signals in remote-Health systems, e-Payment/Voting in smart city. Hence, preserving the confidentiality of data becomes imperative in both commercial and military applications [1], where threats arise from two main aspects, namely security and privacy. Traditional research has focused on secure design for averting eavesdropping, where the aim is to prevent confidential information from being exploited by external eavesdroppers

Zhongxiang Wei is with the College of Electronic and Information Engineering, Tongji University, Shanghai, China. Email: z_wei@tongji.edu.cn

Christos Masouros is with the Department of Electronic and Electrical Engineering at the University College London, London, U.K. Email: c.masouros@ucl.ac.uk

H. Vincent Poor is with the Department of Electrical and Computer Engineering, Princeton University, Princeton, NJ, USA. Email: poor@princeton.edu

Athina P. Petropulu is with the Department of Electrical and Computer Engineering, Rutgers University, NJ, USA. Email: athinap@rutgers.edu

L. Hanzo is with the School of Electronics and Computer Science, University of Southampton, Southampton, U.K. Email: lh@ecs.soton.ac.uk

(Eve)s. Hence, there is extensive literature on cryptography, authentication, multiple-input and multiple-output (MIMO) beamforming, artificial noise, cooperative jamming, and radio frequency fingerprinting, spanning from the upper layers to the physical layer (PHY) of networks [2] [3] [4]. These extensive security-related solutions facilitate secure communications among legitimate parities, while ensuring that the signals cannot be captured by external Eves.

Naturally, cyber-threats also jeopardize privacy. While the data carried in emerging applications is becoming more personal, privacy leakage pervades all applications that require a user to release data in order to receive utility. In general, there are two design principles in privacy protection, i.e, masking data itself or part of it, or concealing the users' identities for the intended receiver. The former line of research seeks to control information leakage, and strikes a compromise between privacy and utility, where mutual information is used as a privacy measure from the perspective of information theory [1]. Similarly, divergence-based metrics such as the variation distance between the a *priori* and a *posteriori* distributions of the disclosed data are used as information leakage measures in the design of differential privacy [5].

A separate line of research focuses on guaranteeing the communication quality towards legitimate parties, while concealing the senders' identities during communication. This is known as anonymous communication [6]. A typical example of anonymous communication is found in cloud/edge computing, where the users wish to get their personal data processed at the cloud or edge. Nevertheless, it is expected that the receiver at the edge, i.e., the access point (AP), only processes the data without the capability of extracting the user's identity, such as his/her name, account, and other unique user-specific information. Another example appears in e-Health applications, where patients wish to anonymously share their physiological information, but all the private information, such as the patients' identities, must remain unknown at the receiver of the medical applications. Similar demand can be also found in anonymous e-Payment/Voting. In a nutshell, anonymity-preserving techniques, where the receiver should only be able to process the data without the knowledge of the users' identities and participation, have become imperative in modern communications.

At the upper layers of networks, a curious receiver may be able to extract the associated user ID during the authentication and encryption processes, or observe the user-specific characteristics of data traffic along the routing path to infer the real identity of the sender. Accordingly, the existing
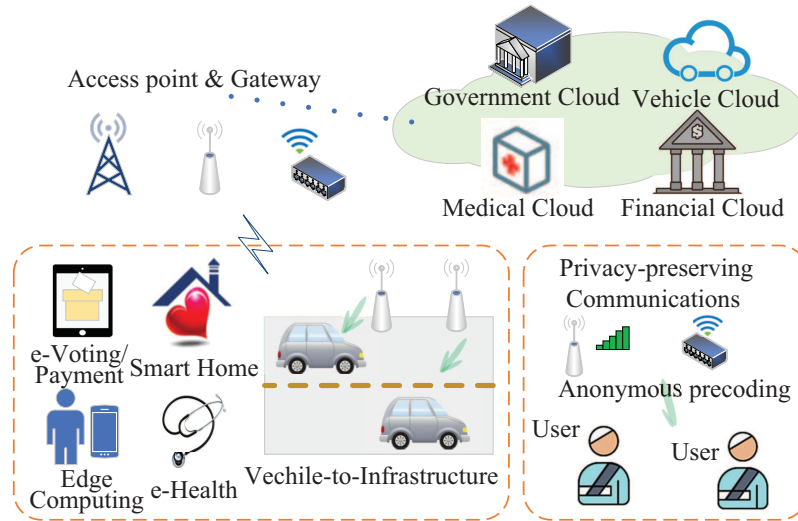
Fig. 1. In emerging applications, a high level of senders' anonymity is preferable through the upcoming paradigm of privacy-preserving techniques at the PHY. This new family of anonymous precoding techniques have been developed to mask senders' identities against the receiver's sender detection behavior, and meanwhile guarantee high receiver-side quality for communication.

anonymity-preserving techniques that reside at upper layers can be classified into anonymous authentication, anonymous encryption and anonymous routing protocols, which are briefly summarized in Table I. Higher layer anonymous authentication and encryption schemes have been proposed for cellular networks, Radio Frequency IDentification [6], wireless body area networks [7], vehicle-to-infrastructure communications and for prototype design [8]. The design philosophy of upper layer anonymous authentication/encryption is to apply group/ring signatures or anonymous account indices [7] for authentication, as well as for constructing communication links and encryption. Since the users only share their so-called pseudo accounts with the service provider, their real IDs are not exposed. In this way, a potential adversary remains unaware of the users real identities and hence fails to identify them. On the other hand, the fundamental principle of anonymous routing is to conceal the user as well as the related routing paths via a number of encrypted layers, relying on an onion-structure; this structure has found wide applications in the Internet and ad-hoc networks [9]. It is striking that, while numerous PHY solutions exist for security, there is a dearth of PHY solutions for anonymity.

Higher layer anonymizing techniques have some drawbacks restricting their practical implementations, i.e.,

- Since the existing anonymous authentication/encryption schemes generally rely on public-key encryption, asymmetric encryption, identity-based encryption, fully homomorphic encryption, cryptographic primitive, etc., they require additional key distribution, agreement and maintenance processes. This may be restrictive in many emerging scenarios due to their excessive complexity and latency. Although small keys have been proposed based on elliptic curve cryptosystems, the communicating parties still need to verify the certificates of others, and a pool

of certificates is required by the certification authority for storing the legitimate parties keys.
- The existing anonymous routing protocols require help from external cooperative agents/routers. The prolonged routing path and the data re-directing mechanism inevitably increase latency. Also, since the anonymous routing protocols give trust to the cooperators along the routing path, they may be vulnerable to internal attacks by curious cooperating members. Further, the cooperators need to stay online during the underlying process thus consuming power.
- As the existing anonymous authentication, encryption and routing designs are designated for the upper layers, they assume that a privacy-preserving link has been established at the PHY. In fact, the hitherto neglected PHY contains critical information that can be analyzed for extracting the senders' identities. For example, when an anonymously authenticated/encrypted user sends a signal via its wireless channel, the receiver can analyze the signalling patterns of the received signal. Based on the channel fading characteristics, the receiver may be able to determine the origin of the signal.

Lack of defense at the PHY may compromise the sender's privacy. Hence, using complementary anonymity-preserving techniques that reside at the PHY is important. However, attaining PHY anonymity is particularly challenging, as it entails the conflicting aims of, on one hand, ensuring high signal quality for data detection at the receiver, and on the other hard, ensuring that the identity of the sender remains hidden from the same receiver. The objective of this article is to introduce the emerging field of PHY anonymity. Commencing from the fundamentals of PHY anonymity, we discuss the issues of sender detection and how it can be applied at the receiver to break the sender's anonymity. Subsequently, the corresponding

TABLE I
A Brief Summary of The Existing Research, from the Perspectives of Security and Anonymity.

Categories	Design Principles	Techniques	Implemented Layers	Pros	Cons
Security (information eavesdropping)	Preventing the confidential signal from being intercepted and decoded by **external** eavesdroppers	Application layer authentication/enciphering	Application layer	i) Based on well-developed symmetric cryptosystems; ii) Not relying on system configuration, i.e., number of antennas and channel diversity	i) High computational complexity; ii) Key distribution/ management are vulnerable to attacks; iii) Relying on the limitations of Eves' computational capacity;
		Network layer authentication	Network layer		
		WiFi protected access	Transport layer		
		Secure socket layer / transport layer security protocols			
		MAC address authentication	MAC layer		
		MIMO beamfomrring	Physial layer	i) No need for secret key distribution/ management; ii) Security can be quantified precisely	Need multiple antennas
		Artificial noise			Additional power on artificial noise
		Cooperative jamming			Need external cooperative nodes
Anonymity	i) Guaranteeing the communication quality of the legitimate parities, ii) and also masking the specific **internal** legitimate parties' identifies during communication	Onion routing protocol	Application layer	Hop-by-hop encryption/ decryption	i) High computational complexity and latency; ii) None of cooperative proxies can be off-line; iii) Vulnerable to internal unhonest members; iv) Ignoring the fundamental threats at the physical layer;
		Network layer routing, such as ANODR, MASK routing protocol	Network layer		
		Certificateless Anonymous Authentication		Use certificateless signature as cryptographic primitive	
		Multi-round Anonymous Authentication		Identifying violator by the times of showing credential	
		Mutual authentication	Link layer	Providing users' location privacy	

anonymous precoding to be used at the sender side is reviewed, followed by a range of open challenges and our conclusions.

II. PERFORMANCE METRIC AND FUNDAMENTALS OF ANONYMITY

Anonymity can be quantified by an entropy-based metric [10]. Assuming that there are K possible senders whose channels towards the receiver are known, the receiver estimates for each potential user k a probability of being the real sender. The highest level of anonymity is achieved when all possible senders are equally probable, resulting in the maximal anonymity entropy. To break the sender's anonymity, the receiver should correctly declare the real sender with a high probability, while computing low probabilities for all other potential senders. On the other hand, at the sender side, an appealingly simple anonymity-preserving technique is to manipulate the transmitted waveform, so that the sender-detection error rate (DER) at the receiver deteriorates, which will be detailed in Section IV. Naturally, anonymity should be achieved without any loss of the reception quality.

Since the users wish to communicate with the receiver in an anonymous manner, they could transmit data without notifying the receiver of their identities, such as their MAC/IP addresses. Hence, the receiver would have knowledge of the received signal only. Before the receiver would attempt to extract the origin of the received signal, it would have to first sense the presence of an incoming signal. The detection of the signal's presence would rely on ubiquitous signal-to-noise ratio (SNR), eigenvalue or feature based energy detector, which has been widely investigated in cognitive radios to sense the availability of spectrum. Once an incoming signal is sensed, the receiver would apply its detection scheme to identify the sender.

III. SENDER DETECTION STRATEGY

Let us consider a typical uplink multiuser MIMO, where the receiver and users are equipped with multiple antennas. Regardless of the precoders applied at the sender, the transmitted signal propagates through the wireless channel, which is a unique, user-specific PHY identity of the specific sender, before it reaches the receiver. Hence, under the time-division-multiple-access premise, the detection of the sender's identity is equivalent to the identification of the propagation channel of the received signal. Since the recipient has sensed the amplitude and phase of the received signals originating from a specific member of the set $\mathbb{K}$, sender detection can be formulated as a multiple hypothesis testing (MHT) problem. In particular, each possible sender is associated with a specific hypothesis.

Considering non-line-of-sight transmission experiencing flat-fading on each carrier, since the receiver has knowledge
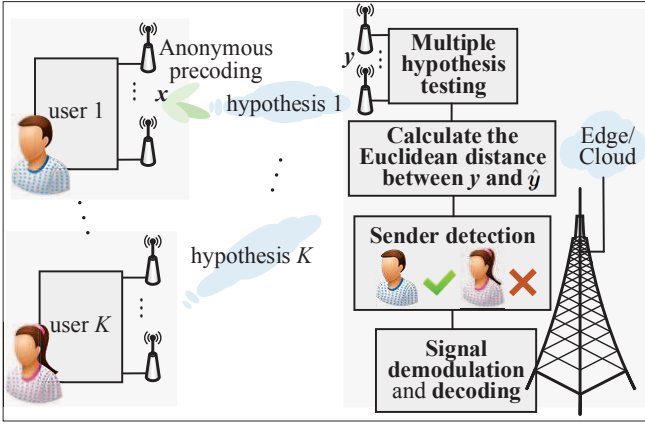
Fig. 2. A generic receiver-side signal processing thread by the curious receiver, where sender detection is performed to unmask the real sender using a multiple hypothesis test.

of channel state information (CSI) of the possible senders, the receiver can estimate the transmitted vector x (which is also the precoded signal at the sender) by multiplying the received signal with the pesudo-inverse of a hypothesized channel. Then, the estimated version of the transmitted signal is left-multiplied by the hypothesized channel to imitate that it propagates through the hypothesized MIMO channel, resulting in a re-constructed signal $\hat{y}$. If the received signal indeed had propagated through the channel considered, the re-constructed signal based on the hypothesized channel would have the smallest Euclidean distance from the real received signal. Motivated by the above observations, the receiver's detection strategy is outlined as follows. The receiver first estimates the transmitted vector and constructs the hypotheses $\hat{y}$ relying on all the possible candidates' channels. Finally, the hypothesis having the smallest Euclidean distance to the actual signal is declared as the real sender [11]. This Euclidean distance based detection relies on the disparity of the small-scale channel fading among the potential senders. However, there are scenarios, for example in high-frequency (e.g., millimeter wave) regimes, where even if some users are closely spaced, their small-scale fading are different, and thus the receiver can unveil the sender with high probability.

The above approach shows that, using the signal propagation model and knowledge of the channel, the receiver can determine who the sender is, in a fashion that is completely independent from the decryption at higher layers. In other words, although the transmitted data can be anonymously authenticated/encrypted at higher layers by the sender, the receiver is able to directly unveil the sender at the PHY [11]. To this end, the classical precoders are no longer anonymous in nature, allowing a leakage of the sender's identify at the PHY. For example, by the well-known singular value decomposition (SVD), signal-to-interference-plus-noise ratio (SINR) balancing, and transmission power minimization precoders, the additional step of channel equalization has to be performed at the receiver for de-modulation. Since a receiver-side equalizer exploits the knowledge of the real sender's channel, this knowledge can be leveraged by the receiver to extract the

sender's identity.

IV. ANONYMOUS PRECODING DESIGN

Now, we examine the family of anonymous precoding techniques that are applied at the sender to hinder the receiver's detector.

The aim of an anonymous precoder is to conceal the sender's identity, and at the same time provide high reception quality [12]. Note that the anonymous precoding technique may be viewed as an outer layer of the existing group/ring signature and anonymous account index based privacy preservation techniques. Explicitly, the existing techniques allocate users pseudo-IDs for authentication, as well as for constructing links and encryption, while anonymous precoding directly improves privacy preservation during communication phase. Interestingly, implementing sender anonymity conflicts with the design of the receiver-side equalizer, which can be proven via the following counter example. If the communication quality can be enhanced by the receiver-side equalizer, no anonymity can be achieved, as the equalizer exploits the real sender's channel. On the other hand, if anonymity is guaranteed and the sender's identity is masked, the receiver is unable to determine the correct propagation channel, indicating that receiver-side equalization is impossible. Hence, the receiver will have to directly demodulate and decode the per-antenna multiplexed data without a reception equalizer; here the MIMO channel between the sender and receiver acts as a multiuser multiple-input and single-output (MISO) channel, as we have to treat each antenna of the receiver individually and consider per-antenna SINR constraint for multiplexing data streams. In the following, we review a pair of anonymous precoder designs [11] [12].

A. Interference Mitigation Based Anonymous Precoder

The philosophy of the interference mitigation (IM)-based anonymous precoder is that of manipulating the transmitted waveform for masking the user-specific information (e.g., CSI) during data transmission, and at the same time strictly suppressing the inter-antenna interference (IAI) using the techniques of suppressing the multi-user interference in MISO systems [11] for communication. All active users send pilot signals to the AP and channel estimation is performed at the AP during training phase. Then the CSI is fed back to the users to be used for precoder design, as in generic MIMO communications. Although the AP can know the users' CSI in its cell, it does not jeopardize the anonymity aims, as the anonymous precoder still succeeds in preventing the AP/server from linking the data received to correct user ID and CSI during communication phase.

Indeed there has been extensive research on anonymity-agnostic MISO precoder design, relying on total power minimization under minimum SINR requirement, SINR balancing under power budget constraints, maximization of the total energy-efficiency under per-user SINR constraint, etc [13]. These problem formulations are generally given as convex or non-convex second order cone programming (SOCP) exercise,
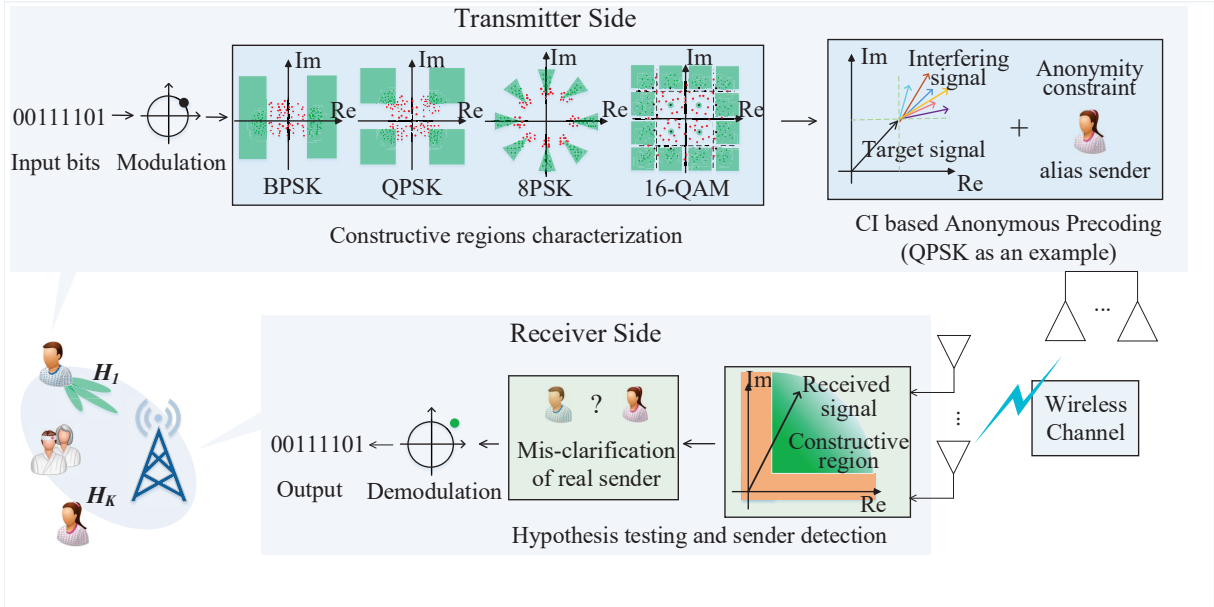
Fig. 3. A generic CI anonymous precoder guideline. At the sender, CI regions are first exploited, and then the symbols are precoded under the CI and anonymity constraints. At the receiver, the users are tested as equally suspicious senders, and hence the sender detection is disabled. Furthermore, since the per-antenna received signal falls into CI regions (green area), conventional demodulation and decoding can be directly performed to obtain the output.

where the resultant problem can be mathematically transformed and handled by semi-definite programming (SDP). When considering the senders' anonymity, an additional anonymity constraint should be imposed on the precoder. Again, the receiver first re-constructs the different hypotheses and considers the one having the smallest Euclidean distance to the actually received signal as the real sender. Hence, to preserve anonymity, the sender can randomly select another candidate from the set $\mathbb{K}$ as an alias sender. That is, the anonymous precoder needs to be appropriately designed to guarantee that the re-constructed signal based on the alias's channel is equivalent to the signal corresponding to the real sender's channel. As a result, the real sender and the alias become equally likely senders from the receiver's perspective, and hence the receiver fails to declare the correct one. The anonymity constraint imposed is linear in nature, which can be simply incorporated in a conventional MISO precoder without breaking the convexity of the problem formulation [12]. Hence, the anonymous precoder can be readily obtained, which guarantees a high reception quality while preserving the anonymity of the sender.

B. Interference Exploitation Based Anonymous Precoding

In the above section, we have discussed the fundamentals of the IM-based anonymous precoder, where the inter-antenna interference is considered as a harmful element that degrades the system performance. As a result, the IM-based precoder has to restrict the received symbols within a certain region around the nominal point in the signal constellation. In fact, the idea of suppressing inter-antenna interference is only optimal from a statistical perspective, where the input is considered as an infinite-cardinality Gaussian signal and only the spatial correlation of the wireless channels is exploited.

However, since the symbols to be transmitted are known by the sender, we can jointly exploit the spatial correlation among the channels and the intended symbols, based on the concept of constructive interference (CI) [14]. Hence, the inter-antenna interference has the potential to be exploited as a useful element to push the per-antenna received symbol away from the detection thresholds of the signal constellation. The resultant increased distance with respect to (w.r.t) the detection threshold directly benefits the per-antenna reception quality. Let us first demonstrate the concept of CI, and then exploit it for our anonymous precoder design.

1) Constructive Interference Based Precoding: We illustrate a generic CI-based anonymous precoder design in Fig. 3 for both binary phase shift keying (BPSK), as well as for quadrature phase shift keying (QPSK), and quadrature amplitude modulation (QAM), etc. First, given the constellation adopted, interference characterization can be performed. The CI regions of each constellation are denoted by the green areas of Fig. 3. To be specific, given the decision boundaries of each modulation constellation, the interference is said to be constructive if it pushes the desired signals away from the decision boundaries while it is said to be destructive if it pulls the signal close to or even across the decision boundaries. For example, the decision thresholds are the real and imaginary axes for QPSK, and hence the interference becomes beneficial if it pushes the desired signals away from both the real and imaginary axes. The characterization of the CI regions can be defined for higher order modulations, such as 8PSK and 16QAM [15], in a similar vain. Hence, we are able to make the IAI always beneficial, where the per-antenna received signal is directly shifted within the CI regions. By utilizing the inter-antenna interference as a beneficial element, the reception quality can be further improved over that of the IM-based precoder.
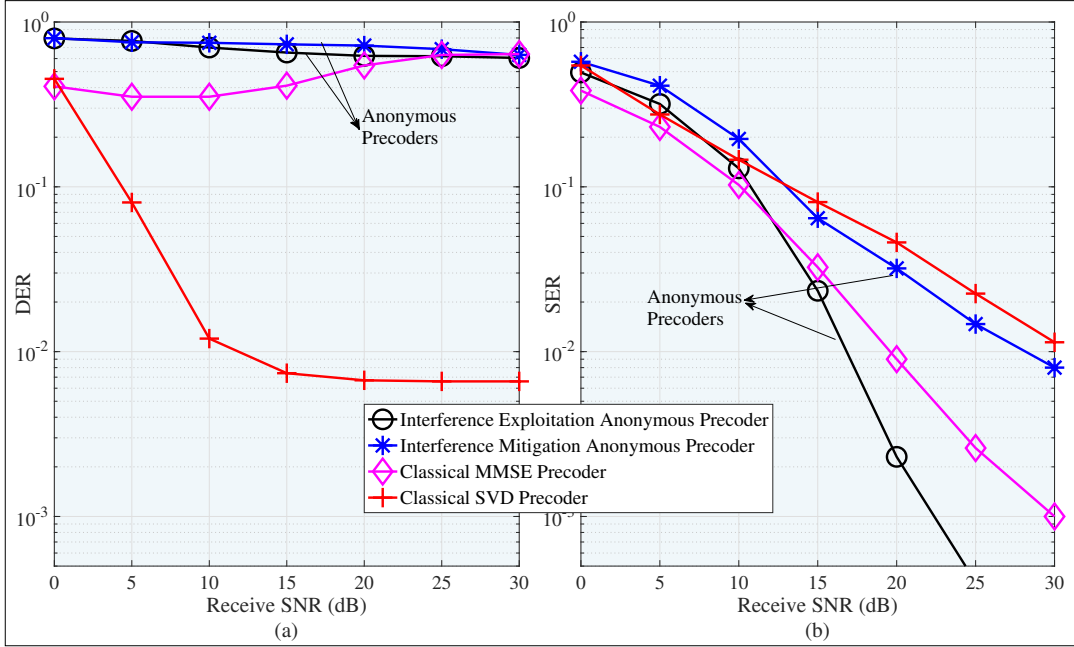
Fig. 4. (a) Anonymous precoders scramble the receivers detection for preserving the senders anonymity, leading to a high DER at the receiver. (b) Low SER is also guaranteed by the anonymous precoders compared to the benchmarks [12].

2) CI Based Precoding with Anonymity Constraint: A key advantage of the CI-based precoding w.r.t anonymity is that, since the received signal is directly shifted into the CI regions, the receiver can simply demodulate the signal, based on its amplitude and phase. As a result, the need for channel equalization at the receiver-side is removed, and there is no need to identify the user's channel that would reveal the sender identity. Hence, the foundation of the CI-based precoding is particularly well suited for anonymous transmission, which is also able to exploit the IAI interference as a helpful component without loss of anonymity.

For illustration, Fig. 3 portrays a generic CI-based anonymous precoder. For employing CI preserving the sender's anonymity, it is essential to impose an additional anonymous constraint to manipulate the pattern of the received signal to mask the sender's PHY characteristics, as we discussed for the IM-based anonymous precoder. In fact, it has been exhibited that the CI precoder itself is a linear precoder, and the CI-related optimization is generally convex in nature [15]. Hence, imposing an additional convex anonymity constraint does not break the convexity and the feasibility of the optimization.

C. Comparative Evaluation

In Fig. 4, the DER and symbol error rate (SER) vs. the SNR trends are demonstrated, benchmarked by the MMSE and SVD precoders [13]. We assume that the hypothesis set $\mathbb{K}$ includes 5 candidate users, where the sender in each time slot (block) is randomly generated. The senders and receiver are equipped with 10 antennas. The power budget is 1 Watt and QPSK modulation is used. It is observed that both the IM and IE anonymous precoders can provide anonymity for the sender, where the receivers DER is as high as 0.8 at high

receive SNRs. By contrast, the SVD precoder shows the worst anonymity performance, as the receiver is able to identify the correct sender with a 0.01 DER at 10 dB SNR. For the MMSE precoder, the receivers DER exhibits a gentle trough. This is because at low receive SNRs, its detection performance is impaired by strong noise, but at high receive SNRs the operation of the MMSE precoder is reminiscent of that of the ZF precoder. Because no CSI knowledge is relied upon, anonymity is incidentally preserved. In Fig. 4(b), since the IE-based anonymous precoder is capable of exploiting the IAI as a desired component, the high DoFs at the sender results in an excellent SER performance, achieving 14 dB SNR gain over the standard MMSE and SVD precoders. Furthermore, the IM-based anonymous precoder can be generally designed by SDP optimization, which is known to have good performance at moderate/high SNRs. Hence, the IM-based anonymous precoder exhibits an SER close to that of the SVD precoder within the 0-12 dB SNR range, while in the region above 12 dB SNR, it outperforms the SVD precoder by about 3 dB. Thus, the anonymous precoders strike an attractive trade-off by providing high communication performance, while preserving the senders anonymity.

Note that since additional anonymity constraints are required for the design of IM-based and IE-based anonymous precoders, the improved anonymity is achieved at the cost of reduced DoFs in precoder design. More importantly, the design principle of the anonymous precoding technique is to manipulate the transmitted waveform for masking the senders identity-related information. Since it does not require help from external proxies, nor does it rely on complex networking or dedicated data re-routing protocols, anonymous precoding techniques are readily applicable to small-scale networks that

have simple architectures and protocols.

V. Open Challenges and Future Research

PHY Anonymity Design with Practical Issues: Practical implementations always suffer hardware impairments, and acquiring accurate CSI may be difficult. All these imperfections would jeopardise the grade of anonymity, which are particularly pronounced in wearable sensors of e-Health applications, or portable devices of edge computing, that are built with low-cost devices. Some pioneering impairment-aware secure PHY solutions do exist, but they cannot be directly applied for anonymous systems. The validation of anonymous precoding considering the above practical issues needs further research.

The Interplay between Anonymity and Data Security in Heterogeneous Networking: The massive number of communication devices results in heterogeneous networks, including but not limited to WBAN, sensor networks, edge/cloud computing, etc. As mentioned in the Introduction, anonymity and data security have distinct objectives and design principles, while in practices, different users and applications may have heterogeneous anonymity and data security specifications. This requires the design of dedicated algorithms for studying the underlying trade-off between anonymity and data security.

PHY Anonymity with Ultra Reliability and Low Latency Applications: Some emerging applications, such as augmented reality and haptic communications, require ultra-reliability and low-latency (i.e., URLLC), where short packet transmission has been considered as a key technique of meeting the stringent requirements of URLLC applications. Evidently, the joint optimization of anonymity, reliability, and latency is nontrivial, which may incur high complexity and overheads. How to preserve PHY anonymity without loss of reliability and increasing latency at acceptable degrees of complexity and overhead, remains an open challenge.

PHY Anonymity from the Perspective of Intelligent Receiver: Providing that abundant computing capability is attainable, the receiver is able to detect the signal sender with the aid of machine learning (ML), which may be hence regarded to as an intelligent-receiver. Leveraging the concept of ML, an intelligent-receiver can analyze the statistics of the signal and develop an ML-enabled detection mechanism, thus improving its detection performance. Thus, it is necessary to reconsider the anonymizing designs of intelligent-receivers.

VI. CONCLUSIONS

This article has discussed the privacy-preserving techniques at the PHY, aiming to provide a comprehensive overview for the concept of PHY anonymity. Starting from the fundamentals of PHY anonymity, we first have discussed the methodology of the sender detection at the receiver, which enables the receiver to disclose the sender by only analyzing PHY information. Subsequently, we have examined the corresponding anonymous precoders to provide the sender's anonymity while guaranteeing a high receive-quality for communication. The reviewed anonymous precoders judiciously manipulate the signalling pattern to scramble the receiver's malicious detection

behavior without harming the convexity and feasibility of precoding design, offering a broad field of preserving anonymity for the privacy-critical applications. Finally, a number of challenges on PHY anonymity are envisaged.

References

[1] M. Bloch *et al.*, "An overview of information-theoretic security and privacy: metrics, limits and applications," *IEEE J. Sel. Inf. Theory*, vol. 2, no. 1, pp. 5-22, Mar. 2021.

[2] L. Dong *et al.*, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. on Signal Process.*, vol. 58, no. 3, pp. 1875-1888, Mar. 2010.

[3] D. Roy *et al.*, "RFAL: Adversarial learning for RF transmitter identification and classification," *IEEE Transa. on Cogn. Commun. Netw.*, vol. 6, no. 2, pp. 783-801, Jun. 2020.

[4] L. Xiao *et al.*, "Reinforcement learning-based PHY authentication for controller area networks," *IEEE Trans. Inf. Forensics Secur.*, vol. 16, no. 1, pp. 2535-2547, Jan. 2021.

[5] Y. Y. Shkel *et al.*, "Secrecy by design with applications to privacy and compression," *IEEE Trans. Inf. Theory*, vol. 67, no. 2, pp. 824-843, Feb. 2012.

[6] M. Chen, S. Chen, and Y. Fang, "Lightweight anonymous authentication protocols for RFID systems," *IEEE/ACM Trans. Networking*, vol. 25. no.3, pp. 1475-1488, Mar. 2017.

[7] J. Liu *et al.*, "Certificateless remote anonymous authentication schemes for wireless body area networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 2, pp. 332-342, Feb. 2014.

[8] K. Emura *et al.*, "Secure and anonymous communication technique: formal model and its prototype implementation," *IEEE Trans. Emerging Topics Comput.*, vol. 4, no. 1, pp. 88-101, Mar. 2016.

[9] K. Sakai *et al.*, "On anonymous routing in delay tolerant networks," *IEEE Trans. Mobile Comput.*, vol. 18, no. 12, pp. 2926-2940, Dec. 2019.

[10] C. Chou *et al.*, "An efficient anonymous communication protocol for peer-to-peer applications over mobile Ad-hoc networks," *IEEE J. Sel. Areas Commun.*, vol. 25, no. 1, pp. 192-203, Jan. 2007.

[11] Z. Wei, F. Liu, C. Masouros, and H. V. Poor, "Fundamentals of physical layer anonymous communications: sender detection and anonymous precoding," *IEEE Trans. Wireless Commun.*, DOI: 10.1109/TWC.2021.3093722

[12] Z. Wei, F. Liu, and C. Masouros, "Physical layer anonymous communications," in *Proc. IEEE GLOBECOM'20*, pp. 1-6, Dec. 2020.

[13] A. Li and C. Masouros, "Interference exploitation precoding made practical: optimal closed-form solution for PSK modulations," *IEEE Trans. Wireless Commun.*, vol. 17, no. 11, pp. 7661-7676, Jan. 2018.

[14] C. Masouros *et al.*, "Known interference in the cellular downlink: a performance limiting factor or a source of green signal power?" *IEEE Commun. Mag.*, vol. 51, no. 10, pp. 162-171, Oct. 2013.

[15] Z. Wei *et al.*, "Multi-cell interference exploitation: enhancing the power efficiency in cell coordination," *IEEE Trans. Wireless Commun.*, vol. 19, no. 1, pp. 547-562, Jan. 2020.

Zhongxiang Wei received his Ph.D. degree in electrical and electronics engineering from the University of Liverpool, Liverpool, U.K., in 2017. From March 2016 to March 2017, he was with the Institute for Infocomm Research, Agency for Science, Technology and Research, Singapore, as a Research Assistant. From March 2018 to March 2021, he was with the department of electrical and electronics engineering, University College London, as a research associate. In April 2021, he joined Tongji University as an associate professor. His interests include PHY anonymity and MIMO systems design. He has served as a symposium/special issue co-chair/TPC member of IEEE ICC, GLOBECOM, and ICASSP.

Christos Masouros is the Professor of Electrical and Electronic Engineering at UCL. He received his PhD in Electrical and Electronic Engineering from the University of Manchester, UK (2009). He has held a Royal Academy of Engineering Research Fellowship (2011-2016). His interests include wireless communications and signal processing with speciality on Large Scale Antenna Systems and Interference Exploitation. He is an Editor for IEEE TWC/TCOM, and has been an Associate/Guest Editor for IEEE COML/JSTSP. He was the recipient of the Best Paper Awards in the IEEE GLOBECOM'15 and WCNC'19.

H. Vincent Poor is the Michael Henry Strater University Professor at Princeton University, where he has been on the faculty since 1990. Prior to joining Princeton, he was on the faculty of the University of Illinois at Urbana-Champaign. He has also held visiting positions at several other universities, including most recently at Berkeley and Cambridge. His research interests are in the areas of information theory, machine learning and network science, and their applications in wireless networks, energy systems and related fields. Among his publications in these areas is the forthcoming book Machine Learning and Wireless Communications, to be published by Cambridge University Press. Dr. Poor is a member of the National Academy of Engineering and the National Academy of Sciences and is a foreign member of the Chinese Academy of Sciences, the Royal Society, and other national and international academies. He received the IEEE Alexander Graham Bell Medal in 2017.

Athina P. Petropulu is a Distinguished Professor of Electrical and Computer Engineering at Rutgers University. Her interests include radar signal processing and PHY security. She received the Presidential Faculty Fellow Award (1995) from NSF and the US White House, and the 2012 IEEE Signal Processing Society (SPS) Meritorious Service Award. She is IEEE and AAAS Fellow. She is co-author of the 2005 IEEE Signal Processing Magazine Best Paper Award, the 2020 IEEE SPS Young Author Best Paper Award and the 2021 Aerospace and Electronic Systems Society Barry Carlton Best Paper Award. She is currently President-Elect of the IEEE SPS.

Lajos Hanzo (http://www-mobile.ecs.soton.ac.uk, https://en.wikipedia.org/wiki/Lajos_Hanzo) (FIEEE'04) received his Master degree and Doctorate in 1976 and 1983, respectively from the Technical University (TU) of Budapest. He was also awarded the Doctor of Sciences (DSc) degree by the University of Southampton (2004) and Honorary Doctorates by the TU of Budapest (2009) and by the University of Edinburgh (2015). He is a Foreign Member of the Hungarian Academy of Sciences and a former Editor-in-Chief of the IEEE Press. He has served several terms as Governor of both IEEE ComSoc and of VTS. He is also a Fellow of the Royal Academy of Engineering (FREng), of the IET and of EURASIP.