PHYSICAL LAYER ANONYMOUS COMMUNICATIONS: AN ANONYMITY ENTROPY ORIENTED PRECODING DESIGN

Zhongxiang Wei †, *Christos Masouros* ‡ *and Sumei Sun* ⋆

† College of Electronic and Information Engineering, Tongji University, Shanghai, China
‡ Department of Electronic and Electrical Engineering, University College London, London, UK
⋆ Institute of Infocomm Research, Agency for Science, Technology and Research, Singapore.

ABSTRACT

Different from traditional security-oriented designs, the aim of anonymizing techniques is to mask users' identities during communication, thereby providing users with unidentifiability and unlinkability. The existing anonymizing techniques are only designated at upper layers of networks, ignoring the risk of anonymity leakage at physical layer (PHY). In this paper, we address the PHY anonymity design with focus on a typical uplink scenario where the receiver is equipped with more antennas than the sender. With the increased degrees-of-freedom at the receiver side, we first propose a maximum likelihood estimation (MLE) signal trace-back detector, which only analyzes the signaling pattern of the received signal to disclose the sender's identity. Accordingly, an anonymity entropy anonymous (AEA) precoder is proposed, which manipulates the transmitted signalling pattern to counteract the receiver's trace-back detector and meanwhile to guarantee high receive signal-to-interference-plus-noise ratio for communication. More importantly, more data streams can be multiplexed than the number of transmit antennas, which is particularly suitable for the strong receiver configuration. Simulation demonstrates that the proposed AEA precoder can simultaneously provide high anonymity and communication performance.

Index Terms— Signal Trace-back Detection, Anonymous Precoding, Physical Layer Anonymity, Strong Receiver

1. INTRODUCTION

In the era of big data, threats arise from two aspects, namely security and privacy [1]. The target of security is to keep the signal unbreakable towards external adversaries [2], and a series of secure techniques have also been proposed, including but not limited to encryption [3], authentication [4], secure precoding [5], artificial noise [6], and other systematic secure protocols, from the upper layers to the PHY layer of the networks. Nevertheless, in the emerging edge/cloud computing and storage, users need to disclose its data towards trusted but curious receivers, in order to receive utility [7]. Hence, departing from the conventional secure design, the aim of privacy protection is to mask part of data [8], or conceal users' identities during communication [9] [10]. The latter one, which is the focus of this work, is known as anonymous communications. An example of the anonymous communications arises from e-Health communications, where patients wish to get their physiological signal analyzed by the medical edge, with the patients' identities kept unknown.

Though a number of anonymizing approaches has been proposed, from the media access control (MAC) layer to the application layer, there are still open challenges. i) The anonymous authentication and encryption techniques [11] [12] use pseudo ID or anonymous account index, instead of the users' real IP/MAC addresses, for user authentication and data encryption. As a result, the curious receiver is unable to identify the origin of the received signal during authentication and encryption. However, they are only able to mask users' identities during authentication and data encryption at the upper layers, ignoring the threat in the subsequent signal transmission phases. ii) The agent-based anonymous protocols deploy external cooperative nodes for data relaying, such as the well-known onion router [13] [14], where the receiver is unaware of the signal source and routing paths. However, its anonymity is breakable by the agents along the routing path. iii) The threat of identity-leaking at the PHY has not been addressed. This threat starts from the acquisition of signal. Since the PHY contains critical information that can be utilized to extract the users' identities, the receiver can analyze the signaling patterns to unmask the users at the PHY directly. PHY layer anonymizing techniques have been investigated in our previous work [9]. A strong sender case was considered, where the receiver has less antennas than the users. Due to the low degrees-of-freedom (DoF)s at the receiver, the detection error rate (DER) of the signal trace-back detector demonstrates a strong error floor (Fig. 1 in Ref. [9]). In practice, the receiver usually has more antennas than the users at uplink, and thus a higher DoF for detection enables a more accurate signal trace-back mechanism, making the provision of the user's anonymity more challenging.

To address the challenges, in this paper we investigate the signal trace-back detection and its counterpart anonymous precoder with the strong receiver configuration, where the main contributions are summarized as follows. i) Focusing on the strong receiver configuration at uplink, we first propose a maximum likelihood estimation (MLE) based signal track-back detector. It only exploits the PHY information of the received signal to break the sender's anonymity, and the DER performance of the MLE based detector is significantly enhanced over that in [9]. ii) To counteract the receiver's enhanced detection performance, we further propose a novel anonymity entropy based anonymous (AEA) precoder, which manipulates the dissipated signaling pattern and meanwhile provides high receive signal-to-interference-plus-noise-ratio (SINR) for communication. To be specific, based on the concept of interference exploitation, the intended signal is designated to be located at constructive regions, instead of being in the proximity region around the constellation point. Hence, it enables multiplexing more data streams than the number of transmit antennas, and also utilizes inter-antenna interference as a beneficial element to enhance receive quality without loss of the sender's anonymity.

2. SYSTEM MODEL AND ANONYMITY METRIC

We consider a multiple-input and multiple-output (MIMO) system at uplink, where K users anonymously transmit signals to an access point (AP) without revealing their identities. The AP is equipped with N_r receive antennas while each user has N_t transmit antennas ($N_r > N_t$). In the training phase, all the active users send pilot signals to the AP and channel estimation is performed at the AP side; then the channel state information (CSI) is fed back to the users for use in precoding design, as that in generic MIMO communications. It is important to note however that the CSI estimation process does not jeopardize the anonymity aims of our work. It is because the aim of our work is to obstruct the AP, that has all users' IDs, from linking the data received to the correct user ID. Assume a time-division-multiple-access fashion and the k-th user as the sender without loss of generality [15]. Define $\boldsymbol{H}_k \in \mathbb{C}^{N_r \times N_t}$ as the MIMO channel between the k-th user and AP, $\boldsymbol{W}_k$ as the precoder, and $\boldsymbol{s}_k$ as the symbols to be transmitted. The received signal at the AP is given by

$$\boldsymbol{y} = \boldsymbol{H}_k \boldsymbol{W}_k \boldsymbol{s}_k + \boldsymbol{z}, \tag{1}$$

where $\boldsymbol{z} \sim (\boldsymbol{0}, \sigma^2 \boldsymbol{I}_{Nr})$ denotes the Gaussian noise at the AP.

Anonymity can be quantified by an entropy-based metric [16], which in fact measures the uncertainty of a system. Define a set $\mathbb{K} = |K|$, and let p_k denote the probability that the AP estimates the k-th user as the real sender. Hence, the anonymity entropy can be calculated as $\mathcal{A}(\mathbb{K}) = -\sum_{k\in\mathbb{K}} p_k \log_2 p_k$. Evidently, a favorable anonymous precoder needs to inhibit the AP's detection, while guaranteeing reasonable SINR quality for communication. In the following, we will first design the signal trace-back detector at the AP in Section III, and then the anonymous precoder at the sender is given in Section IV.

3. SIGNAL TRACE-BACK DETECTOR DESIGN

The signal trace-back detection is formulated as a multiple hypotheses testing (MHT) problem at the AP-side, given by

$$\mathcal{Y} = \begin{cases} \mathcal{H}_0 : & \boldsymbol{z}, \\ \mathcal{H}_1 : & \boldsymbol{H}_1 \boldsymbol{W}_1 \boldsymbol{s}_1 + \boldsymbol{z}, \\ \quad \vdots & \\ \mathcal{H}_K : & \boldsymbol{H}_K \boldsymbol{W}_K \boldsymbol{s}_K + \boldsymbol{z}, \end{cases} \tag{2}$$

where the hypothesis $\mathcal{H}_0$ means that only noise exists, while hypothesis $\mathcal{H}_k$ means the presence of a signal sent from the k-th user. Evidently, the AP can first detect the hypothesis $\mathcal{H}_0$, and only clarifies the origin of the signal if $\mathcal{H}_0$ is decided as a false hypothesis. The clarification of $\mathcal{H}_0$ leads to a classic energy detection with the test statistic $\mathcal{T}(\boldsymbol{y}) = \frac{||\boldsymbol{y}||^2}{N_r}$, which is compared against a threshold β for declaring the presence of an incoming signal. Define the probability of false alarm as the probability of the AP falsely clarifying the presence of an incoming signal. The probability of false alarm is calculated as $P_{FA}(\beta|\mathcal{H}_0) = 1 - F_{(2N_r)}(\frac{2\beta N_r}{\sigma^2})$, where $F_{(2Nr)}(\cdot)$ denotes the cumulative distribution function (cdf) of a chi-square random variable with $2N_r$ DoFs. There is a series of other energy detectors, and we refer readers to [17] for the discussion herein. Subsequently, the AP can turn to clarify the origin of the signal. Since the propagation channel is the unique PHY identity of a specific user within certain time, the detection of the sender's identity is equivalent to the identification of the propagation channel. With the knowledge of CSI set $\boldsymbol{H}_k, \forall k \in \mathbb{K}$, the AP is able to apply the MLE to estimate the transmitted vector $\boldsymbol{x}_k = \boldsymbol{W}_k \boldsymbol{s}_k \in \mathbb{C}^{N_t \times 1}$, in the form as $\hat{\boldsymbol{x}}_k = \boldsymbol{H}_k^\dagger \boldsymbol{y} = \boldsymbol{W}_k \boldsymbol{s}_k + \boldsymbol{H}_k^\dagger \boldsymbol{z}$, where $\boldsymbol{H}_k^\dagger = (\boldsymbol{H}_k^H \boldsymbol{H}_k)^{-1} \boldsymbol{H}_k^H$ denotes the pseudo-inverse of the channel $\boldsymbol{H}_k$. Then, the estimated vector $\hat{\boldsymbol{x}}_k$ is left multiplied by $\boldsymbol{H}_k$ to imitate that it propagates through MIMO channel $\boldsymbol{H}_k$, leading to a re-constructed signal $\hat{\boldsymbol{y}}_k$ as $\hat{\boldsymbol{y}}_k = \boldsymbol{H}_k \hat{\boldsymbol{x}}_k = \boldsymbol{H}_k \boldsymbol{W}_k \boldsymbol{s}_k + \boldsymbol{H}_k \boldsymbol{H}_k^\dagger \boldsymbol{z}$. Evidently, if the received signal comes from the k-th user, there is a high probability that the re-constructed signal $\hat{\boldsymbol{y}}_k$ built on $\boldsymbol{H}_k$ has the smallest Euclidean distance to the actual signal $\boldsymbol{y}$. Hence, the AP can calculate the Euclidean distance between the actual signal and different re-constructed signal in sequence, and clarify the one with the minimum value as the real sender. Finally, the MLE-based signal trace-back detector is finally written as

$$\mathcal{D}^*_{MLE} = \min_{k\in\mathbb{K}} \{||(\boldsymbol{I}_{N_r} - \boldsymbol{H}_1 \boldsymbol{H}_1^\dagger)\boldsymbol{y}||^2, ..., ||(\boldsymbol{I}_{N_r} - \boldsymbol{H}_K \boldsymbol{H}_K^\dagger)\boldsymbol{y}||^2\}, \tag{3}$$

Note that $\boldsymbol{H}_k \boldsymbol{H}_k^\dagger \neq \boldsymbol{I}_{N_r}$ when $N_r > N_t$. In our previous work [9], the so-called MHT detector was proposed, which demonstrates a strong DER error floor (we refer readers to [9] for the discussion herein). In contrast, the MLE detector is able to clarify the real sender with a low level of DER, which will be shown in our simulation part. As a result, a great challenge is imposed for the sender's anonymous precoder design against the AP's detection.

4. ANONYMITY ENTROPY BASED PRECODER

Problem formulation of the anonymous precoder design and its optimal solution are presented in subsections IV-A and B.

4.1. Problem Formulation

By the MLE detector, since the AP calculates the norm in (3) in sequence and considers the one with the minimum value as the sender, we can select another user k', $k' \neq k$, from the set $\mathbb{K}$ as an alias, and confines the following inequality as

$$||(\boldsymbol{H}_{k'}\boldsymbol{H}_{k'}^{\dagger} - \boldsymbol{H}_k\boldsymbol{H}_k^{\dagger})\boldsymbol{H}_k\boldsymbol{W}_k\boldsymbol{s}_k||^2 \leq \delta, \forall k' \neq k, k' \in \mathbb{K}, \quad (4)$$

With a small-valued threshold δ, (4) lets the k-th and k'-th users equally suspicious to the AP, and hence the AP fails to declare who is the real sender as well as the exact channel that the signal comes from, further indicating that a correct equalizer would be impossible. Hence, we need to treat each receive antenna of the AP as an individual receiver and guarantee per-antenna SINR requirement for multiplexing data streams, so that the AP can decode the signal directly without the help of the channel equalizer. Note that the principle is to manipulate the dissipated signal pattern to inhibit the AP's detection, instead of letting the alias k' transmit artificial noise. Now, we target to maximize the per-antenna SINR under the sender's anonymity entropy requirement, written as

$$\begin{aligned} &P1 : \max_{\boldsymbol{W}_k} \ \Gamma, \\ &\text{s.t. (C1)} : ||\boldsymbol{W}_k\boldsymbol{s}_k||^2 \leq p_{max}, \ \text{(C2)} : \Gamma_r \geq \Gamma, \forall r \in N_r, \\ &\text{(C3)} : ||(\boldsymbol{H}_{k'}\boldsymbol{H}_{k'}^{\dagger} - \boldsymbol{H}_k\boldsymbol{H}_k^{\dagger})\boldsymbol{H}_k\boldsymbol{W}_k\boldsymbol{s}_k||^2 \leq \delta, \forall k' \neq k, k' \in \mathbb{K}, \end{aligned} \quad (5)$$

where (C1) denotes the power budget constraint. (C2) guarantees the per-antenna SINR Γ_r higher than the lower-bound Γ. (C3) suppresses the test norm to inhabit the AP's detection.

4.2. Optimization Solution

The difficulties of solving P1 lie in multiplexing N_r data streams (where $N_r > N_t$), and meanwhile guaranteeing the sender's anonymity requirement. In [9], we have proposed an interference-suppression based anonymous (ISA) precoder, whereas it is only applicable for the strong sender case with $N_r \leq N_t$. More importantly, by the ISA precoder, the transmitted data is considered as Gaussian signal, and thus the inter-antenna interference is always treated as a harmful element to be strictly suppressed, which significantly reduces the DoFs of the precoder design.

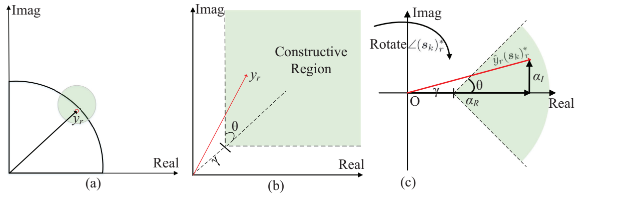

Fig. 1. The conventional precoders locates the intended signal in the proximity region around the constellation point (in Fig. 1(a)). In contrast, the IE-based precoder locates the desired symbol ($\frac{1+i}{\sqrt{2}}$ with QPSK modulation for illustration) into a constructive region (green area in Fig. 1(b)), by exploiting the geometric interpretation in Fig. 1(c).

In practice, the constellation size is limited and the input may not always be Gaussian signal. Since the transmitted symbols are known by the sender, based on the concept of interference exploitation (IE) [18], the inter-antenna interference can be utilized as a beneficial element to enhance the per-antenna receive performance. Let us start by briefly discussing the concept of IE and then we elaborate IE for addressing anonymity. We use PSK modulation for notation simplicity, nevertheless the following is applicable to multi-level modulations [19]. Write the intended symbol of the r-th receive antenna as $(\boldsymbol{s}_k)_r = de^{j\phi_r}$ by M-PSK modulation, where the symbol amplitude is normalized to $|d| = 1$. It can be expressed as a rotated version of another symbol, such that $(\boldsymbol{s}_k)_r = (\boldsymbol{s}_k)_{r'}e^{j(\phi_r - \phi_{r'})}$. Denotes $\boldsymbol{w}_r \in \mathbb{C}^{N_r \times 1}$ as the precoder vector for the intended symbol $(\boldsymbol{s}_k)_r$, where we have $\boldsymbol{W}_k = [\boldsymbol{w}_1^T, ...\boldsymbol{w}_r^T, ..., \boldsymbol{w}_{N_r}^T]^T$ and $\boldsymbol{s}_k = [(\boldsymbol{s}_k)_1, ..., (\boldsymbol{s}_k)_r, ..., (\boldsymbol{s}_k)_{N_r}]$. Hence, the received signal of the r-th receive antenna is written as

$$y_r = \boldsymbol{h}_r \sum_{r'=1}^{N_r} \boldsymbol{w}_{r'}(\boldsymbol{s}_k)_r e^{j(\phi_{r'} - \phi_r)} + z_r, \quad (6)$$

where $\boldsymbol{h}_r \in \mathbb{C}^{1 \times N_r}$ denotes the channel from the sender to the r-th receive antenna, and z_r is the noise at the r-th receive antenna. Taking s_1 as a reference symbol (which can be arbitrary), the received signal is re-written as $y_r = \boldsymbol{h}_r e^{j(\phi_1 - \phi_r)} \sum_{r'=1}^{N_r}(\boldsymbol{w}_{r'}e^{j(\phi_{r'} - \phi_1)})(\boldsymbol{s}_k)_r + z_r$, which denotes that the original inter-antenna interference channel reduces to a virtual multicast channel with common messages $(\boldsymbol{s}_k)_r$ to all receive antennas [19], and hence the inter-antenna interference can be turned into a beneficial element. Write $\hat{y}_r$ as the noise-excluded signal on the r-th receive antenna. To make the inter-antenna interference constructive, one can rotate $\hat{y}_r$ with an angle $\angle(\boldsymbol{s}_k)_r^*$, and then the rotated signal can be mapped onto imaginary axis $\alpha_r^{\Im} = \Im\{\hat{y}_r(\boldsymbol{s}_k)_r^*\}$ and real axis $\alpha_r^{\Re} = \Re\{\hat{y}_r(\boldsymbol{s}_k)_r^*\}$, respectively. As shown in in Fig. 1(c), $\hat{y}_r$ falls into a constructive region (in Fig. 1(b)) if and only if $|\alpha_r^{\Im}| \leq (\alpha_r^{\Re} - \gamma)\tan(\frac{\pi}{M})$ holds, where M denotes constellation size. In particular, γ physically denotes the Euclidean distance in the signal constellation between the constructive region and the decision thresholds, which directly relates to SINR performance. Substituting $\alpha_r^{\Im}$ and $\alpha_r^{\Re}$ into the inequality above yields

$$
\begin{aligned}
&|\Im\{\boldsymbol{h}_r \boldsymbol{W}_k \boldsymbol{s}_k (\boldsymbol{s}_k)_r^*\}| \leq \\
&(\Re\{\boldsymbol{h}_r \boldsymbol{W}_k \boldsymbol{s}_k (\boldsymbol{s}_k)_r^*\}) - \gamma_r)\tan(\frac{\pi}{M}),
\end{aligned}
\tag{7}
$$

Now, P1 can be readily transformed into an equivalent optimization problem

$$
\begin{aligned}
&P2: \max_{\boldsymbol{W}_k} \gamma, \text{ s.t. (C1)}: ||\boldsymbol{W}_k \boldsymbol{s}_k||^2 \leq p_{max}, \text{ (C2)}: (7), \forall r \in N_r, \\
&\text{(C3)}: ||(\boldsymbol{H}_{k'} \boldsymbol{H}_{k'}^{\dagger} - \boldsymbol{H}_k \boldsymbol{H}_k^{\dagger}) \boldsymbol{H}_k \boldsymbol{W}_k \boldsymbol{s}_k||^2 \leq \delta, \forall k' \neq k, k' \in \mathbb{K}.
\end{aligned}
\tag{8}
$$

Though P2 is standard convex problem, if one selects all the $k' \in \mathbb{K}$ as aliases (hence there are K-1 constraints in (C3)), all the users will be equally suspicious to the AP with the highest level of anonymity $\mathcal{A}(\mathbb{K}) = \log_2 K$. Nevertheless, it significantly constrains the DoFs for precoder design, further degrading the per-antenna SINR performance. To make a good compromise between the communication SINR and sender's anonymity, we can randomly select a user k' from $\mathbb{K}$ as the alias. As a result, there will be only 1 constraint in (C3) without significantly confining DoFs. Also, the AP still fails to declare the correct sender, as the sender k and the alias k' are equally suspicious. The whole algorithm is finally summarized as follows.

Algorithm 1 The AEA Precoder Design

```
Input: CSI $\boldsymbol{H}_k$, power budget $p_{max}$, intended symbol $\boldsymbol{s}_k$.
1: Select a random user $k'$ from $\mathbb{K}$ as the alias. Then solve P2.
Output: Optimal precoding design $\boldsymbol{W}_k^*$.
```

Remark 1: Based on the AEA precoder, the received signal of each antenna has been directly located into constructive regions of the constellation. Hence, the AP can demodulate the received signal based on the amplitude and phase of the received signal. As a result, it removes the need for receiver or transmitter equalization, while utilizing inter-antenna interference as a beneficial element without loss of anonymity.

5. SIMULATION RESULTS

Now, we present the simulation results. Each block includes 50 symbols, and Rayleigh block-fading is adopted for channel modeling. The following classic precoders are selected as comparison algorithms: 1) IE precoder [20], where the sender's anonymity is not considered. 2) MMSE precoder [21]. 3) SVD precoder [22]. In particular, the AP first tries to reveal the real sender, and then the precoder and equalizer are calculated based on the declared hypothesis. Note that the ISA precoder in [9] is not plotted as it is inapplicable for the strong receiver configuration.

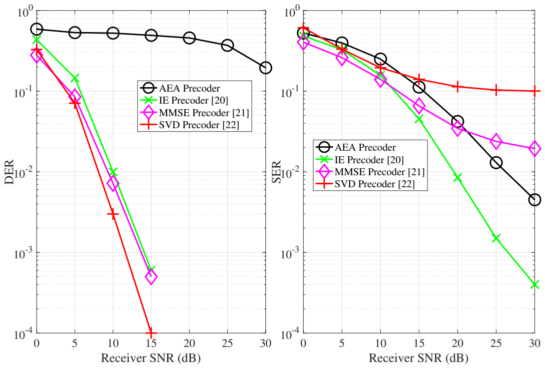

Fig. 2. DER and SER performance vs. different receive SNRs, where $\delta = 0.03$, $N_r = 10$, $N_t = 9$, K=5, $p_{max} = 1$ Watt, and $\beta = 10^{-2}$. QPSK modulation is adopted.

As can be observed in Fig. 2, since the AEA precoder controls the pattern of the waveform to scramble the AP's signal trace-back detector, the AP's DER is pushed to a high level, thereby ensuring the sender's anonymity. In comparison, with the conventional SVD, MMSE and IE precoders, the AP is able to reveal the correct sender with a low DER performance, i.e., DER=10^{-3} at 15 dB SNR regime. On the other hand, since the IE precoder utilizes the inter-antenna interference without anonymous constraints, its high DoFs endorse the lowest SER performance [20]. However, the proposed AEA precoder achieves a close SER to the IE precoder, and outperforms the SVD and MMSE at moderate/high SNR regimes. Hence, the AEA precoder makes a good compromise between guaranteeing reasonable receive quality for communication and providing senders anonymity.

6. CONCLUSIONS

Focusing on the strong receiver configuration at uplink, we first have proposed a novel MLE signal trace-back detector for the AP, which only analyzes the signaling patterns of the received signal to disclose the sender's identity and demonstrates a significantly enhanced detection ability. Accordingly, we have further proposed a AEA precoder to provide anonymity for the sender, and simultaneously maintain high per-antenna SINR performance for communication. In particular, the AEA precoder is able to multiplex more data streams than the number of the transmit antennas. Compared to the classic IE, MMSE, SVD precoders, simulation results have demonstrated that the proposed AEA precoder can scramble the AP's anonymity-violating detector, where the DER of is pushed to a high level. Also, high per-antenna receive SINR is guaranteed, striking a good compromise between the anonymity and communication performance.

7. REFERENCES

[1] R. Khan, P. Kumar, D. N. K. Jayakody, and M. Liyanage, “A survey on security and privacy of 5G technologies: potential solutions, recent advancements, and future directions,” *IEEE Commun. Survey Tut.*, vol. 22, no. 1, pp. 196–248, Jan. 2020.

[2] Y. Wu, A. Khisti, C. Xiao, G. Caire, K. K. Wong, and X. Gao, “A survey of physical layer security techniques for 5g wireless networks and challenges ahead,” *IEEE J. Sel. Areas Commun.*, vol. 35, no. 4, pp. 675–695, Apr. 2018.

[3] S. Liu, J. Yu, Y. Xiao, Z. Wan, S. Wang, and B. Yan, “BC-SABE: block chain-aided searchable attribute-based encryption for cloud-IoT,” *IEEE Internet Things J.*, vol. 7, no. 9, pp. 7851–7867, Sept. 2020.

[4] C. Lyu, D. Gu, Y. Zeng, and P. Mohapatra, “PBA: prediction-based authentication for vehicle-to-vehicle communications,” *IEEE Trans. on Dependable and Secure Comput.*, vol. 13, no. 1, pp. 71–83, Jan. 2016.

[5] Z. Wei and C. Masouros, “Device-centric distributed antenna transmission: secure precoding and antenna selection with interference exploitation,” *IEEE Internet Things J.*, vol. 7, no. 3, pp. 192–203, Mar. 2020.

[6] Z. Wei, C. Masouros, and F. Liu, “Secure directional modulation with few-bit phase shifters: optimal and iterative-closed-form designs,” *IEEE Trans. Commun.*, vol. 69, no. 1, pp. 486–500, Jan. 2021.

[7] K. Kalantari, L. Sankar, and A. D. Sarwate, “Robust privacy-utility tradeoffs under differential privacy and hamming distortion,” *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 11, pp. 2816–2830, Nov. 2018.

[8] M. Bloch, O. Gunlu, A. Yener, F. Oggier, H. V. Poor, L. Sankar, and R. F. Schaefer, “An overview of information-theoretic security and privacy: metrics, limits and applications,” *IEEE J. Sel. Areas Inf. Theory*, vol. 2, no. 1, pp. 5–22, Mar. 2021.

[9] Z. Wei, F. Liu, and C. Masouros, “Physical layer anonymous communications,” in *Proc. IEEE GLOBECOM’20*, Dec. 2020, pp. 1–6.

[10] Z. Wei, C. Masouros, H. V. Poor, A. P. Petropulu, and L. Hanzo, “Physical layer anonymous precoding: the path to privacy-preserving communications,” *to appear in IEEE Wireless Commun.*, 2021.

[11] B. Lian, G. Chen, M. Ma, and J. Li, “Periodic k-times anonymous authentication with efficient revocation of violator’s credential,” *IEEE Trans. Inf. Forensics Secur.*, vol. 10, no. 3, pp. 543–557, Mar. 2015.

[12] K. Emura, A. Kanaoka, S. Ohta, K. Omote, and T. Takahashi, “Secure and anonymous communication technique: formal model and its prototype implementation,” *IEEE Trans. Emerging Topics Comput.*, vol. 4, no. 1, pp. 88–101, Jan. 2015.

[13] “Tor project [online]. available: http://www.torproject.org/,” *accessed date Feb. 20*, 2015.

[14] K. Sakai, M. Sun, W. Ku, and J. Wu, “On anonymous routing in delay tolerant networks,” *IEEE Trans. Mobile Comput.*, vol. 18, no. 12, pp. 2926–2940, Dec. 2019.

[15] S. Ali, N. Rajatheva, and W. Saad, “Fast uplink grant for machine type communications: challenges and opportunities,” *IEEE Commun. Mag.*, vol. 57, no. 3, pp. 97–103, Mar. 2019.

[16] Z. Wei, F. Liu, C. Masouros, and H. V. Poor, “Fundamentals of physical layer anonymous communications: sender detection and anonymous precoding,” *to appear in IEEE Trans. Wireless Commun.*, 2021.

[17] E. Axell, G. Leus, E. G. Larsson, and H. V. Poor, “Spectrum sensing for cognitive radio: State-of-the-art and recent advances,” *IEEE Signal Process. Mag.*, vol. 19, no. 4, pp. 101–116, Apr 2012.

[18] C. Masouros, T. Ratnarajah, M. Sellathurai, C. B. Papadias, and A. K. Shukla, “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.

[19] Z. Wei, C. Masouros, K. K. Wong, and X. Kang, “Multi-cell interference exploitation: enhancing the power efficiency in cell coordination,” *IEEE Trans. Wireless Commun.*, vol. 19, no. 1, pp. 547–562, Jan. 2020.

[20] 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, Sept. 2018.

[21] C. B. Peel, B. M. Hochwald, and A. L. Swindlehurst, “A vector-perturbation technique for near-capacity multi-antenna multiuser communication—part i: channel inversion and regularization,” *IEEE Trans. Wireless Commun.*, vol. 53, no. 1, pp. 195–202, Jan. 2005.

[22] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*, 2nd ed. Cambridge, U.K: Cambridge University Press, 2005.