IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 31 January 2023, accepted 14 February 2023, date of publication 28 February 2023, date of current version 7 March 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3250251

RESEARCH ARTICLE

IRS-Assisted Physical Layer Security for 5G Enabled Industrial Internet of Things

BAKHTIAR ALI[1], JAWAD MIRZA[1], (Senior Member, IEEE), SAJID HUSSAIN ALVI[2], MOHAMMAD ZUBAIR KHAN[3], MUHAMMAD AWAIS JAVED[1], (Senior Member, IEEE), AND ABDULFATTAH NOORWALI[4]

[1]Department of Electrical and Computer Engineering, COMSATS University Islamabad, Islamabad 45550, Pakistan
[2]Department of Physics, COMSATS University Islamabad, Islamabad 45550, Pakistan
[3]Department of Computer Science and Information, Taibah University, Medina 42353, Saudi Arabia
[4]Department of Electrical Engineering, Umm Al-Qura University, Mecca 21961, Saudi Arabia

Corresponding author: Jawad Mirza (jaydee.mirza@gmail.com)

The authors extend their appreciation to the Deputyship for Research & Innovation, Ministry of Education in Saudi Arabia for funding this research work through the project number : IFP22UQU4290235DSR257.

ABSTRACT 5G is a key enabler of Industrial Internet of Things (IIoT) that provides seamless connectivity between machines, sensors and computing servers. Security and privacy are major concerns for 5G enabled IIoT. Physical Layer Security (PLS) is a promising technique that can enhance the security of 5G enabled IIoT. In this paper, we present an IRS-assisted PLS scheme for 5G enabled IIoT that improves the weighted secrecy sum-rate (WSSR) of the industrial wireless network, where eavesdroppers are present around the facility. The key idea is to jointly optimize active and passive beamforming vectors to increase the secrecy rate at the user. To maximize WSSR, we use the stable matching algorithm that optimally assigns IRSs for secure data sharing between industrial units. Simulation results show that the proposed scheme enhances the WSSR performance by 40% and minimum secrecy rate by 25% as compared to the random and maximum weight matching schemes, respectively.

INDEX TERMS Omni-IRS, MISO, secrecy rate, stable matching.

I. INTRODUCTION

Reliable and secure connectivity of sensor devices, industrial machines and cloud servers is a major component of Industry 4.0 [1], [2], [3]. Industrial Internet of Things (IIoT) will provide robust wireless communications among industrial units, thus a fully automated and smart factory concept can be realized [4], [5], [6], [7]. This has many applications for process control, machine health monitoring, predictive maintenance, and enhanced decision making based on real-time machine data.

There are two main ingredients of a reliable and secure IIoT system. The first one is the error free data sharing among the IIoT nodes. This means that data is shared with extremely high reliability under different wireless channel and network load conditions [7]. The second one is the secure and privacy aware communication mechanism for the IIoT network. This refers to meeting confidentiality, integrity and availability security requirements of data communications [8], [9], [10].

To achieve the above two requirements of a reliable IIoT system, 5G standard provides many advanced features such as high data rate transmission using massive Multiple-Input Multiple-Output (MIMO), enhanced throughput using intelligent beamforming, improved coverage using Device-to-Device (D2D) communications, and better use of available spectrum using full-duplex communications [11].

While the above features of 5G technology can improve the overall system performance, they may fail to provide extreme reliability needed for many applications such as autonomous driving, and industrial process control [7]. As an example, temperature control in a heat exchanger is critical for many industries. An error in control signal information transmission to heat exchanges from a central server in a 5G enabled IIoT can cause major loss.

The associate editor coordinating the review of this manuscript and approving it for publication was Olutayo O. Oyerinde.

Similarly, privacy and security of data is a vital requirement for 5G enabled IIoT [12], [13], [14]. Internet connected industrial machines are susceptible to cyber attacks by malicious users. For example, attackers can jeopardize an industrial process by eavesdropping critical information share among machines. Malicious nodes can also send jamming signals to capture the network bandwidth, thus not allowing other critical information to be shared among machines. Finally, data integrity attacks can also be carried out by attackers, sharing wrong information about process control, and machine operations.

To mitigate the above challenges, two upcoming technologies can be used by 5G enabled IIoT. The first technology is the Physical Layer Security (PLS) to enhance security and privacy of IIoT. The second technology is Intelligent Reflecting Surfaces (IRS) that can enhance network capacity and also assist in efficient PLS.

PLS is a technique that uses wireless transmission characteristics such as noise and channel conditions, to achieve secure transmission at the intended receiver and reduce the shared information at the eavesdropper [15], [16]. As compared to traditional cryptographic schemes, PLS do not require any security keys and also do not incur delays required for signing and verification of digital signatures [17].

IRS is considered to be a game changing technology which is driven by the growing demands of future wireless networks [18]. IRSs are artificial 2-D planar metasurfaces which are intelligently constructed and have reconfigurable features implemented through electronic circuits. A typical IRS consists of large number of passive-radio antennas also known as reflective-radio elements. With the help of these reconfigurable IRS elements, an impinging electromagnetic wave can be reflected towards the desired direction [19]. This steering of the transmitted signal by programming the reflective elements makes the communication environment smart and controllable. Therefore, an IRS can be used to assist the communication between two nodes to improve the received signal quality and reduce co-channel interference, which in turn increases the spectral efficiency of the network.

Due to its attractive features, IRS has been widely investigated in single-user communication, multi-user communication, wireless power transfer systems, cognitive radio networks, PLS and many other applications. Recently, researchers are investigating the usefulness of IRS technology in challenging environments, such as underwater, underground, industrial and disaster [18]. In industrial environment, IRS can be used to guarantee reliable and low latency communication to achieve massive connectivity requirement set by industry 4.0. Both indoor and outdoor deployment of IRSs can assist industrial communication network. The indoor deployment of IRS in industrial environment and its advantages are explained in [18]. For outdoor industrial environment, IRSs can assist the users which are blocked due to some large obstacles between the communication link. In addition to that, IRS can also provide an efficient PLS solution for security concerns of industrial wireless communication systems, which are raised due to massive connectivity among the densely deployed sensor devices.

Recently, security of IIoT networks has attracted a lot of research attention. It is expected that a significant amount of industrial data and information will flow across 5G networks with high quality (i.e., increased bandwidth and reduced latency) [20]. To enable efficient industrial operations, security of IIoT links is essential. As, IIoT devices are lightweight they are unable to support upper layer cryptographic protocols with large communication overheads. Therefore, PLS and cross-layer security techniques with low communication overheads are more suitable for the deployment of massive IIoT devices.

In this study, we propose the use of multiple omni-IRSs for PLS in an outdoor industrial wireless communication system, where active eavesdroppers are present near the receiving devices. Unlike traditional IRS, omni-IRS is capable of not only reflecting but transmitting the signals to their opposite direction. This feature of omni-IRSs enhances their coverage range as compared to the tradition (reflect only) IRSs [21], [22]. Moreover, we consider multiple-antenna transmitter in order to achieve beamforming gains which are not available in Single-Input Single-Output (SISO) communication links. More precisely, we consider a Multiple-Input Single-Output (MISO) communication system, where each user has single antenna. Due to the presence of an eavesdropper (attacker), we employ efficient active beamforming at the transmitter and passive beamforming at the omni-IRS to maximize the secrecy rate of the user (also referred as Bob). The main idea is to assign each Bob a single IRS, such that the overall Weighted Secrecy Sum Rate (WSSR) of the network is maximized. As the studied problem is one-to-one bipartite matching, we rely on the stable matching algorithm known as Gale-Shapley algorithm for IRS-Bob assignment. The usefulness of the stable matching in our studied problem is that once the assignment process completes, there is no IRS-Bob pair which is better off, if they are allowed to change their assigned partners. The IRS assisted PLS method proposed in this study is not limited to 5G enabled IIoT networks, but it can be employed in IRS aided multiuser MISO communication systems. The main contributions of the work are summarized below:

- We consider multiuser MISO wireless communications for IIoT networks in the presence of multiple eavesdroppers. We propose to use multiple omni-IRSs in the network for PLS. These omni-IRSs are deployed in the surrounding areas which are capable of reflecting the signals in front of the IRS and transmitting the signals to the region behind the IRS. The omni-IRSs are more beneficial than the traditional reflect only IRSs as the network coverage can be improved.
- To secure the communication links from the eavesdroppers, we employ a PLS technique where phase shifts of the omni-IRS are configured to null out the signal at

the eavesdropper. For this purpose, an IRSs assignment problem is formulated as an optimization problem which maximizes the weighted sum secrecy rate (WSSR) of the network.

The paper is organized as follows. Section II provides an overview of recent work in the areas of PLS and IRS-assisted PLS. Section III describes the system model used in the paper. Section IV explains the active and passive beamforming optimization algorithm for PLS. Section V explains the proposed IRS assignment algorithm for PLS in 5G enabled IIoT. Section VI provides a discussion on the simulation results. Section VII presents the conclusions of the paper.

II. RELATED WORKS

In this section, we review the PLS techniques for different IoT networks. We also discuss the recent work related to IRS-assisted PLS.

In [23], authors propose an optimal authentication signal (also known as tag) power algorithm for Physical Layer Authentication (PLA) in IIoT networks. While a high tag transmit power reduces the tag error probability, it also increases message error probability. Therefore, a tradeoff exists in the tag transmit power selection. The proposed technique minimizes the tag error probability under system power constraints. An iterative point based technique is used to select the optimal tag transmit power. Results show that the proposed technique maintains the tag error rate and system power below the required thresholds.

The work in [24] proposes an energy efficient PLS technique for Simultaneous Wireless Information and Power Transfer (SWIPT) and virtual MIMO based IoT. The key idea of the proposal is to achieve PLS using beamforming and jamming. An optimization problem is developed which includes beamforming vector, power and time splitting ratios. Iterative optimization with penalty function is used to solve the above problem. The proposed technique improves the secrecy rate as shown by the results.

The authors in [25] present a learning algorithm for dynamic selection of physical layer attributes for PLS. Attributes are selected using authentication performance history of each attribute. The goal is to select those attributes that reduce false alarms and miss detection rates. A learning algorithm is developed to optimally select the attributes. Simulation results show reduced miss detection rate.

The work in [26] presents an IRS-assisted PLS technique for NOMA users which are out of the coverage range of the Base Station (BS) due to some obstruction. These users are known as dead-zone users. Thus, IRS facilitates the dead-zone NOMA users to communicate with the BS. An Alternate Optimization (AO) algorithm is used to select beamforming and power allocation. The proposed technique maximizes the secrecy rate as highlighted by the simulation results.

To improve the working of PLS for MISO systems, Simultaneously Transmitting and Reflecting Intelligent Reconfigurable Surface (STAR-IRS) is used in [27]. As STAR-IRS can transmit and reflect at the same time, it offers better performance as compared to the simple IRS. For the proposed work, the authors consider three different modes of transmission, i.e., energy splitting, time splitting and mode selection. The proposed technique jointly optimizes the beamforming, transmit and reflection coefficients of IRS. Results show improved secrecy rate when using the proposed technique.

In [28], the secrecy performance of IRS-assisted PLS is investigated. Authors first evaluate the Cumulative Distribution Function (CDF) and Probability Density Function (PDF) of Signal-to-Noise Ratio (SNR) in the presence of IRS. Using these distribution functions, analytical derivations of security metrics such as secrecy outage probability and secrecy rate are provided using stochastic geometry techniques. With IRS-assisted PLS, the secrecy rate is shown to improve as compared to non-IRS based PLS.

The work in [29] investigates the use of Artificial Noise (AN) for PLS. The proposed technique optimizes the transmit precoding matrix at the BS, co-variance matrix for the AN and IRS phase shift values. Block Coordinate Descent (BCD) algorithm is used to maximize the secrecy rate. Results highlight the gain achieved by the proposed BCD algorithm in terms of secrecy rate as compared to other techniques.

III. SYSTEM MODEL

Consider an IIoT network as shown in Fig. 1 where an industrial plant is connected with its industrial processing units. The IIoT connectivity is established using omni-IRSs and a MISO communication system is considered. The transmitter is equipped with M antennas and there are total of L omni-IRSs deployed in the surrounding area. Furthermore, there are K number of total users (also referred as Bob), where each user has single antenna and one active eavesdropper (Eve) is present in its close proximity. The transmitter uses IRSs to serve each user at each time slot based on a Time Division Multiple Access (TDMA). Each omni-IRS consists of N number of passive reflecting/transmitting elements. The omni-IRSs are capable of switching between two modes: transmitting and reflecting [27]. This allows the IRSs to serve users on both sides of the surfaces. In this paper, we assume that the omni-IRS uses time splitting protocol in which it can work in either transmitting mode or reflecting mode at any given time instance. The transmitting or reflecting coefficients of the l^{th} omni-IRS can be expressed as $\Phi_l = \text{Diag}\{e^{j\phi_{1,l}}, e^{j\phi_{2,l}}, \ldots, e^{j\phi_{N,l}}\}$.

The direct link between the transmitter and the users (Bobs) is assumed to be in deep fade, and therefore, absent. The channel between the transmitter and the l^{th} IRS is modeled as Rician fading channel which is given as [27]

$$\mathbf{F}_l = \sqrt{\frac{\kappa_l}{\kappa_l + 1}}\mathbf{F}_l^{\text{LoS}} + \sqrt{\frac{1}{\kappa_l + 1}}\mathbf{F}_l^{\text{NLoS}}, \tag{1}$$

TABLE 1. Recent work related to PLS and IRS-assisted PLS (SWIPT: Simultaneous Wireless Information and Power Transfer, MIMO: Multiple Input Multiple Output, FDD: Frequency Division Duplex, NOMA: Non-Orthogonal Multiple Access, AO: Alternate Optimization, MISO: Multiple Input Single Output, STAR-IRS: Simultaneously Transmitting and Reflecting Intelligent Reconfigurable Surface, BCD: Block Coordinate Descent, AN: Artificial Noise.

Technique	Network	Goal	Key Idea	Results
PLS [23]	IIoT	Authentication signal (tag) power optimization	Minimize tag error probability Interior point method optimization	Improved error rate Improved power
PLS [24]	IoT	PLS for SWIPT and virtual MIMO based IoT	Optimal beamforming, power & time splitting Iterative optimization with penalty function	Improved secrecy rate
PLS [25]	IoT	Dynamic selection of PLS attributes	Attribute selection using past performance Reduce false alarms and miss detection rates	Reduced miss detection rate
PLS & IRS [26]	6G	IRS enabled PLS for dead-zone NOMA users	AO to maximize secrecy rate Optimal beamforming and power allocation	Improved secrecy rate
PLS & IRS [27]	Cellular	STAR-IRS enabled PLS for MISO networks	AO to maximize secrecy rate Optimal beamforming & coefficients of IRS	Improved secrecy rate
PLS & IRS [28]	Cellular	Secrecy performance of IRS assisted PLS	Analytical derivations of PLS using stochastic geometry	Improved secrecy rate
PLS & IRS [29]	Cellular	Use of IRS in artificial noise based PLS	BCD algorithm to maximize secrecy rate Optimal precoding, AN and IRS phase shifts	Improved secrecy rate

where, κ_l is the Rician factor. We represent $\mathbf{F}_l^{\text{LoS}} \in \mathbb{C}^{N\times M}$ and $\mathbf{F}_l^{\text{NLoS}} \in \mathbb{C}^{N\times M}$ as the LoS and NLoS components of the channel between the transmitter and the l^{th} IRS, respectively. Furthermore, we denote $\mathbf{h}_{k,l} \in \mathbb{C}^{N\times 1}$ as the channel between the l^{th} IRS and the k^{th} Bob. Similarly, $\mathbf{g}_{k,l} \in \mathbb{C}^{N\times 1}$ is the channel between the l^{th} IRS and the k^{th} Eve (which is closer to the k^{th} Bob). Here, we assume that both Bob and Eve channels experience Rician fading propagation conditions, and therefore, these channels are also modeled as (1). It is furthermore assumed that channel state information (CSI) of all links is known to the transmitter i.e., perfect global CSI is available at the transmitter. A controller is used at each IRS to manage it from the transmitter [30], which is commonly implemented by a field programmable gate array.

The transmitter sends an independent signal to each user (or Bob) in a TDMA manner. Let us denote s_k as the signal for the k^{th} Bob, with $\mathbb{E}[|s_k|^2] = 1$. Then, the signals received at the k^{th} Bob and associated Eve through the l^{th} omni-IRS can be expressed as

$$y_{k,l}^{\text{b}} = \mathbf{h}_{k,l}^H \Phi_l^H \mathbf{F}_l \mathbf{w}_k \mathbf{s}_k + n_k^{\text{b}}, \tag{2a}$$
$$y_{k,l}^{\text{e}} = \mathbf{g}_{k,l}^H \Phi_l^H \mathbf{F}_l \mathbf{w}_k \mathbf{s}_k + n_k^{\text{e}}, \tag{2b}$$

where, $\mathbf{w}_k \in \mathbb{C}^{M\times 1}$ is the beamforming vector for the k^{th} Bob. The transmit/reflect passive beamforming vector at the l^{th} omni-IRS is given by $\Phi_l \in \mathbb{C}^{N\times N}$. The additive white Gaussian noise (AWGN) at the k^{th} Bob and Eve, served by the l^{th} IRS, are given by n_k^{b} and n_k^{e}, respectively, having variances $\sigma_{\text{b},k}^2$ and $\sigma_{\text{e},k}^2$. Using the transformation in [27], we also define a phase vector as $\boldsymbol{\theta}_l = \text{diag}(\Phi_l)$. Now denoting $\mathbf{H}_{k,l} = \text{Diag}(\mathbf{h}_{k,l}^H)\mathbf{F}_l$ and $\mathbf{G}_{k,l} = \text{Diag}(\mathbf{g}_{k,l}^H)\mathbf{F}_l$, we can re-write (2a) and (2b) as

$$y_{k,l}^{\text{b}} = \boldsymbol{\theta}_l^H \mathbf{H}_{k,l} \mathbf{w}_k \mathbf{s}_k + n_k^{\text{b}}, \tag{3a}$$
$$y_{k,l}^{\text{e}} = \boldsymbol{\theta}_l^H \mathbf{G}_{k,l} \mathbf{w}_k \mathbf{s}_k + n_k^{\text{e}}. \tag{3b}$$

The SNRs for the k^{th} Bob-Eve pair, served through the l^{th} omni-IRS, using (3a) and (3b), can be expressed as

$$\text{SNR}_{k,l}^{\text{b}} = \frac{\left|\boldsymbol{\theta}_l^H \mathbf{H}_{k,l} \mathbf{w}_k\right|^2}{\sigma_{\text{b},k}^2}, \tag{4a}$$
$$\text{SNR}_{k,l}^{\text{e}} = \frac{\left|\boldsymbol{\theta}_l^H \mathbf{G}_{k,l} \mathbf{w}_k\right|^2}{\sigma_{\text{e},k}^2}. \tag{4b}$$

Using above SNR expressions for the k^{th} Bob and Eve pair, we can define the associated secrecy rate as

$$R_{k,l} = \ln\left(1 + \frac{\left|\boldsymbol{\theta}_l^H \mathbf{H}_{k,l} \mathbf{w}_k\right|^2}{\sigma_{\text{b},k}^2}\right) - \ln\left(1 + \frac{\left|\boldsymbol{\theta}_l^H \mathbf{G}_{k,l} \mathbf{w}_k\right|^2}{\sigma_{\text{e},k}^2}\right) \tag{5}$$

The main objective of this study is to leverage omni-IRSs to achieve PLS such that the WSSR performance is maximized. There are two main challenges to this problem. Firstly, the

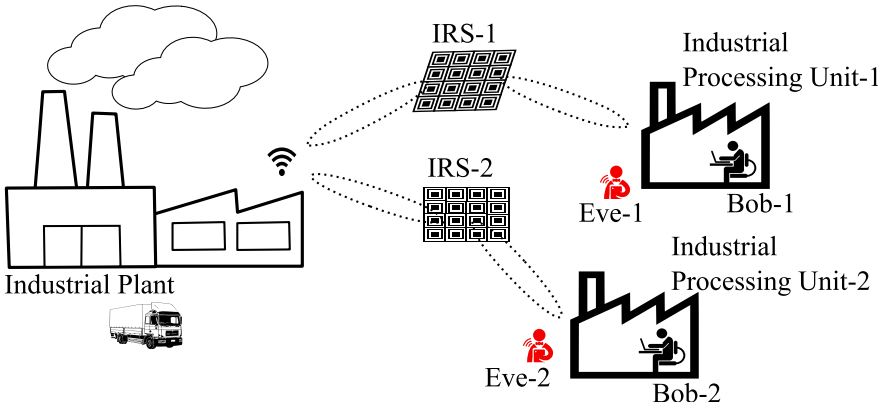

FIGURE 1. Illustration of system model for omni-IRSs assisted IIoT network.

transmitter needs to optimize the active beamforming vector, $\mathbf{w}_k$, and phase shift matrix, Φ_l, for the k^{th} Bob-Eve pair assigned with the l^{th} omni-IRS, such that the secrecy rate is maximized. Secrecy rates for the k^{th} Bob-Eve pair are calculated by assigning it with all the IRSs in an iterative manner. This process is repeated for all the K Bob-Eve pairs present in the network. Secondly, an optimal IRS-Bob-Eve assignment is required, where each omni-IRS is allotted to a single Bob-Eve pair, such that WSSR of the system is maximized. In this work, we assume perfect CSI at the transmitter. However, the beamforming optimization and proposed IRS assignment can be employed with imperfect CSI as well but this will result in the degradation of the secrecy performance. This degrade will depend on the mismatch between the channel and its estimate version.

IV. ACTIVE AND PASSIVE BEAMFORMING OPTIMIZATION

In this section, we present the framework for the joint optimization of active and passive beamforming that maximizes WSSR, which is based on an AO approach presented in [27]. The joint optimization problem to maximize WSSR can be written as [27]

$$\text{(P1)}: \max_{\mathbf{w}_k, \boldsymbol{\theta}_l} \sum_k \alpha_k R_{k,l} \tag{6a}$$

$$\text{s.t.} \quad \sum_k \|\mathbf{w}_k\|^2 \leq P_{\max}, \tag{6b}$$

$$[\theta_l]_n = e^{j\phi_{n,l}}, \ \forall n, \tag{6c}$$

$$\phi_{n,l} \in [0, 2\pi), \ \forall n, \tag{6d}$$

where, $\alpha_k \in [0, 1]$ is the weight for the k^{th} Bob secrecy rate. The weight of the link refers to the priority of the link, i.e., higher the value of the weight, higher will be the priority of that link. $P_{\max}$ is the total transmission power at the transmitter. Here, omni-IRS index l represents the index of the omni-IRS which is assigned to the k^{th} Bob. The matching of omni-IRSs and Bobs are presented in Section V. The problem (P1) presented above for the WSSR maximization has coupled variables. Therefore, it needs to be decoupled using path-following method [27] around given points $\{\widetilde{\mathbf{w}}_k, \widetilde{\boldsymbol{\theta}}_l\}$. Using the problem (P1) transformation given in [27], we can re-formulate the WSSR maximization problem (P1) as problem (P2), as shown at the bottom of the page. In problem (P2), we relax the unit modulus constraint (6c) and (6d) on the phases. As the problem (P2) is convex with a linear constraint, it can be solved using the interior-point method with the help of optimization toolbox CVX. In particular, the resultant phase values obtained by solving the problem (P2) are mapped to the nearest discrete value in the vector $\boldsymbol{\vartheta}$, where $\boldsymbol{\vartheta} = [1, e^{j2\pi/Q}, \ldots, e^{j2\pi(Q-1)/Q}]$ consists of total Q quantized coefficients for the elements of the omni-IRS.

The optimization of active and passive beamforming vectors using the problem (P2) is outlined in Algorithm 1. First, the given points $\{\widetilde{\mathbf{w}}_k, \widetilde{\boldsymbol{\theta}}_l\}$ are set along with the stopping criteria ϵ. In the first iteration (i.e., $t = 0$), the active beamforming vector for the k^{th} Bob, given by $\mathbf{w}_k$, is determined using the problem (P2), while keeping the phase shift vector, $\boldsymbol{\theta}_k$, fixed. In the next step, the active beamforming vector $\mathbf{w}_k$ at $t = 0$ is used to obtain the phase shift vector, $\boldsymbol{\theta}_l$, by solving the

$$\text{(P2)}: \min_{\mathbf{w}_k, \boldsymbol{\theta}_l} \sum_k -\frac{2\alpha_k}{\sigma^2_{\text{b},k}} \Re\left\{\mathbf{w}_k^H \mathbf{H}_{k,l}^H \boldsymbol{\theta}_l \widetilde{\boldsymbol{\theta}}_l^H \mathbf{H}_{k,l} \widetilde{\mathbf{w}}_k\right\} + \frac{\alpha_k \left|\widetilde{\boldsymbol{\theta}}_l^H \mathbf{H}_{k,l} \widetilde{\mathbf{w}}_k\right|^2 \left|\boldsymbol{\theta}_l^H \mathbf{H}_{k,l} \mathbf{w}_k\right|^2}{\left(\sigma^2_{\text{b},k} \left|\widetilde{\boldsymbol{\theta}}_l^H \mathbf{H}_{k,l} \widetilde{\mathbf{w}}_k\right|^2 + \sigma^4_{\text{b},k}\right)} + \frac{\alpha_k \left|\boldsymbol{\theta}_l^H \mathbf{G}_{k,l} \mathbf{w}_k\right|^2}{\left|\widetilde{\boldsymbol{\theta}}_l^H \mathbf{G}_{k,l} \widetilde{\mathbf{w}}_k\right|^2 + \sigma^2_{\text{e},k}} \tag{7a}$$

$$\text{s.t.} \quad \sum_k \|\mathbf{w}_k\|^2 \leq P_{\max}, \tag{7b}$$

Algorithm 1 Optimization of Active and Passive Beamforming Using Problem (P2) Given by (7)

Initialization $t = 0, \widetilde{w}_k, \widetilde{\boldsymbol{\theta}}_l, P_{\max}, \epsilon$

Repeat

1) Obtain $\mathbf{w}_k^{(t)}$ from problem (P2) for fixed $\boldsymbol{\theta}_l^{(t)}$.
2) Use $\mathbf{w}_k^{(t)}$ from (1) to obtain $\boldsymbol{\theta}_l^{(t)}$ from problem (P2).
3) $t \rightarrow t+1$.
4) Update $\mathbf{w}_k^{(t+1)} = \mathbf{w}_k^{(t)}$ and $\boldsymbol{\theta}_l^{(t+1)} = \boldsymbol{\theta}_l^{(t)}$.

Until $R_{k,l}^{(t+1)} - R_{k,l}^{(t)} \leq \epsilon$

Output $\left(\mathbf{w}_k^{(t+1)}, \boldsymbol{\theta}_l^{(t+1)}\right)$.

problem (P2). For the next iteration ($t = 1$), $\mathbf{w}_k$ is computed using the $\boldsymbol{\theta}_l$ obtained in the previous iteration. The process continues till the stopping criteria is satisfied, i.e., there is a small difference between the WSSR values of successive iterations. Note that once the algorithm stops, the entries of the output phase shift vector is mapped to quantized values of $\boldsymbol{\vartheta}$.

V. IRSs ASSIGNMENT PROBLEM

In this section, we present omni-IRSs assignment to Bob-Eve pairs which is based on a popular one-to-one stable matching algorithm known as Gale-Shapley. We assume that the total number of IRSs in the network is equal to the total number of Bob-Eve pairs, i.e., $L = K$. Denoting, $\mathcal{B} = \{b_1, b_2, \ldots, b_K\}$ and $\mathcal{O} = \{o_1, o_2, \ldots, o_K\}$ as the set of Bobs and IRSs, respectively, the aim of this work is to obtain a stable IRS-Bob matching $\mu : \mathcal{B} \rightarrow \mathcal{L}$ that maximizes the WSSR performance of the network, such that

$$\max_{\mu} \sum_{k} \alpha_k R_{k,\mu(k)}, \text{ s.t. } \mu \text{ is a matching}, \tag{8}$$

where $\mu(k)$ denotes the index of the IRS which is matched to the k^{th} user. As the studied problem is one-to-one matching, each Bob will be matched with only one IRS.

It is assumed that the transmitter has perfect CSI available for all the links, therefore, the transmitter computes all the possible Bob-IRS permutations and creates a preference list of each IRS, which is based on secrecy rate of Bobs in descending order. For any given matching μ, the secrecy rate of the k^{th} Bob-Eve pair is given by $R_{k,\mu(k)}^{(\mu)}$. The secrecy rate can be expressed with respect to the l^{th} IRS as $R_{\mu(l),l}^{(\mu)}$, where $\mu(l)$ denotes the index of the Bob-Eve pair which is matched to the l^{th} IRS. Note that in this stage, active and passive beamforming vectors are computed using Algorithm 1 at the transmitter, for all the permutations. Once the calculations are completed for all the possible IRS-Bob permutations, the preference list created by the transmitter for the l^{th} IRS is denoted by PL_IRS$_l$. Unlike the transmitter, the Bob has knowledge of its own local channel only. Therefore, each Bob generates its preference list based on the offered rates from IRSs, which is given by $C_{k,l} = \ln\left(1 + \left|\boldsymbol{\theta}_l^H \mathbf{H}_{k,l} \mathbf{w}_k\right|^2 / \sigma_{\text{b},k}^2\right)$ $\forall\, l$. The preference list at the Bob consists of IRSs indices, which are ranked in a descending order based on their offered rate. We denote the preference list of the k^{th} Bob as PL_Bob$_k$.

Algorithm 2 Gale-Shapley Based IRS Assignment

Input: Set of all Bobs $\mathcal{B}$ and IRSs $\mathcal{L}$, Bob preference lists PL_Bob$_k$ $\forall\, k$, IRS preference lists PL_IRS$_l$ $\forall\, l$

Initialize Each IRS $\in \mathcal{L}$ to be free, $\mu = \emptyset$
while *IRS* $o_l \in \mathcal{L}$ *is free and PL_IRS*$_l \neq \emptyset$ **do**
  b_k = Bob on the top of o_l's list to whom o_l has not proposed yet
  if (b_k is not assigned)
    Assign b_k and o_l to be allocated to each other
    $\mu \leftarrow \mu \cup (b_k, o_l)$
  else if (b_k prefers o_l over previously assigned o_j)
    Assign o_j to be free $\mu \leftarrow \mu/(b_k, o_j)$
    Assign b_k and o_l to be allocated to each other
    $\mu \leftarrow \mu \cup (b_k, o_l)$
  else
    b_k rejects o_l and (o_l remains unassigned)
  end if
end
Output μ: matched IRS-Bob pairs

A. GALE-SHAPLEY

The BS performs the IRS-Bob assignment based on Gale-Shapley algorithm, such that the resultant matching is IRS optimal. The pseudocode of the proposed IRS-Bob matching with Gale-Shapley algorithm is presented in Algorithm 2. If the Bob (which is on the top of the IRS preference list) is not already matched with another IRS, the transmitter allocates this most favoured Bob to the IRS. If the preferred Bob has already been assigned to one of the other IRS, it is only reassigned to the proposing IRS if the Bob also prefers it to the assigned IRS. The same procedure is followed until all IRSs have been matched. There is no alternative matching in which any IRS is better off than others, resulting in a stable matching. After the matching procedure is complete, the transmitter uses Algorithm 1 to compute active and passive beamforming vectors, so that IRSs can reflect or transmit the signal to their assigned Bob-Eve pairs. The complexity of the Gale-Shapley scheme is $O(L^2)$.

The complexity of the whole algorithm is divided into two parts. The first part is obtaining the active and passive beamforming power via the AO algorithm provided in Algorithm 1. The optimization of active and passive beamforming components in Algorithm 1 has the complexity of $O(M^2)$ and $O(N^2)$, respectively. The second part is the IRS assignment process given in Algorithm 2, which has the complexity of $O(L^2)$. For the convergence of the AO algorithm, we refer the reader to [27], where the convergence of Algorithm 1 is numerically validated.

B. MAXIMUM WEIGHT MATCHING

For comparison purposes in Section VI, we use maximum weight matching algorithm. In the maximum weight matching problem, the main objective is to achieve a matching in which the sum of weights (here, WSSR) is maximized. This is achieved by assigning the best Weighted Secrecy Rate (WSR) to the corresponding IRS-Bob pair. Then the next best WSR is selected and associated IRS-Bob pair are matched. This process continues until all the IRSs are matched. The disadvantage of maximum weight matching algorithm is that the Bobs who are assigned with the IRSs near the end of the allocation process will have much lower WSR as compared to the Bobs who were assigned IRSs in the beginning.

C. EXHAUSTIVE SEARCH MATCHING

In exhaustive search, all the IRS-Bob permutations are computed and the best matching is selected in terms of WSSR. This method is computationally complex when the total number of IRS-Bob pairs are large, however, it provides upper bound on the WSSR performace of the network.

D. RANDOM MATCHING

In random matching, the IRS is randomly assigned to the Bob. The WSR are ignored in this matching algorithm, and therefore, it gives a lower bound on the performance of the network.

VI. RESULTS AND DISCUSSION

In this section, we present the numerical results to evaluate the performance of the omni-IRSs assisted industrial communication network for various matching schemes discussed in Section V. We perform MATLAB based Monty Carlo simulation of various algorithms to show the performance comparison. We use MATLAB based CVX tool for solving the joint optimization problem of Algorithm 1. In the simulations we assumed that the transmitter is fixed at the origin $(0, 0)$. The maximum distance between the transmitter and the Bob is denoted by $d_{\max}$, which is selected to be equal to 200 meters. At each channel realization, the location of the Bobs are selected randomly and their distances with the transmitter are restricted within the range of $d_{\max}$. On the other hand, IRSs are deployed uniformly over the y-axis but restricted to be closer to the transmitter.

Each Bob is known to be accompanied by an eavesdropper which is deployed randomly on a circle centered around the Bob with radius ranging from $2-5$ meters. The number of transmit antenna is set to $M = 8$, the transmission power is fixed to $P_{\max} = 10$ dB, the number of IRSs is fixed at $L = 5$, with each IRS consists of $N = 50$ passive elements. The number of Bob-Eve pairs are also selected to be $K = 5$. For fairness, we consider the weights of all the links to be same, i.e., $\alpha_k = 1\ \forall k$. All the parameter defined here are fixed until and unless specified otherwise. We provide results for Rician factor of $\kappa = 3$ dB and $\kappa = 10$ dB for all the channels, while $\sigma^2_{\mathrm{b},k} = \sigma^2_{\mathrm{e},k} = -80$ dBm. The path loss is given by $C_r(d/d_0)^{-\alpha}$, where $C_r = 10^{-3}$ is the path loss at the reference distance of $d_0 = 1$ m and d is the link distance. The path loss exponent is set to $\alpha = 2$. For the Algorithm 1, $\widetilde{\mathbf{w}}_k$ is generated randomly as a complex Gaussian vector, such that $\|\widetilde{\mathbf{w}}_k\| = 1\ \forall k$. Similarly each element of the vector $\widetilde{\boldsymbol{\theta}}_l$, given by $e^{j\widetilde{\theta}_n}\ \forall n$, are generated using random phase from the range $(0, 2\pi]$. The stopping criteria, ϵ, for the Algorithm 1 is set to 0.01.

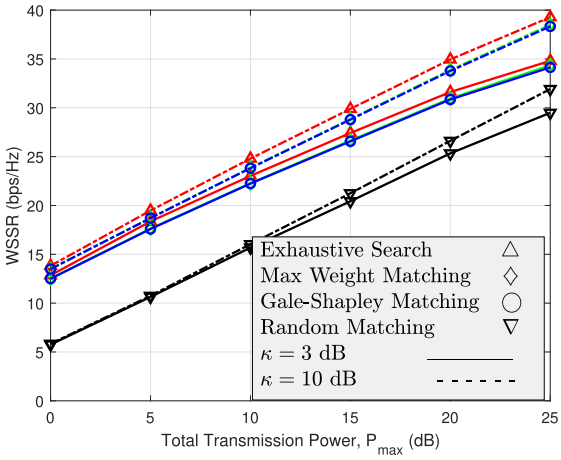

FIGURE 2. The WSSR performance versus total transmission power.

The WSSR performance is shown in Fig. 2 against the range of transmission power values. The WSSR is the sum of all the secrecy rates of the Bobs obtained after the IRS-Bob matching. The transmission power ranges from 0dB to 25dB. Results are evaluated with two different values of the rician factor $\kappa = 3$ and $\kappa = 10$. It can be seen that as the transmission power increases, the WSSR performance also improves. Here, we compare the WSSR performance of the Gale-Shapley based stable matching algorithm with other schemes: exhaustive search, maximum weight matching and random matching. The performance of Gale-Shapley based stable matching algorithm is very close to the upper bounded exhaustive search matching. It is interesting to note that the Gale-Shapley and maximum weight matching schemes give same performance given that the latter does not yield a stable matching. Furthermore, the random matching algorithm performs the worst among all the plotted algorithms.

To further investigate the performance of Gale-Shapley and maximum weight matching algorithms, in Fig. 3 we plot the minimum secrecy rate results against $P_{\max}$ values. This rate corresponds to the secrecy rate of Bob-Eve pair which is the minimum rate among all other pairs. As the Gale-Shapley algorithm yields the stable matching where no IRS-Bob pair is worst off, therefore, it gives better minimum secrecy rate performance as compared to the maximum weight matching algorithm. In fact, the minimum secrecy rate performance with Gale-Shapley is very close to the exhaustive search method. This result justifies the use of stable matching based Gale-Shapley algorithm for IRS-Bob matching.

In Fig. 4, we plot the WSSR results by varying the number of passive elements N in each IRS. Once again, it can be

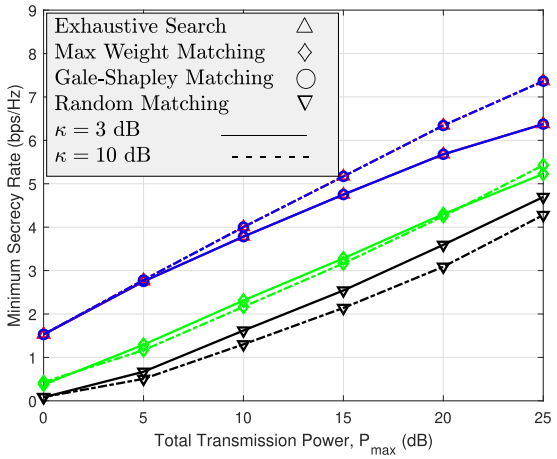

FIGURE 3. The minimum secrecy rate in the network versus total transmission power.

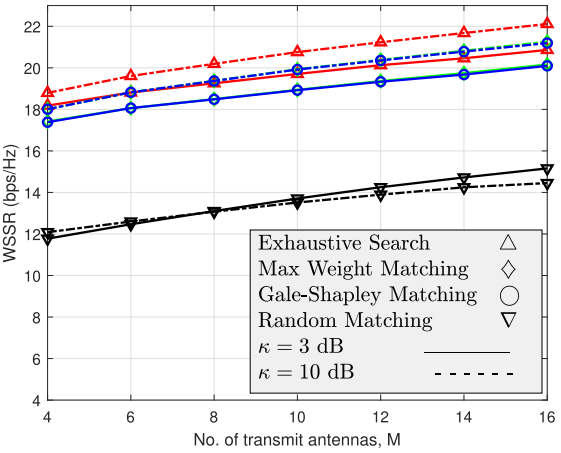

FIGURE 5. The WSSR performance versus the number antennas, M, at the transmitter.

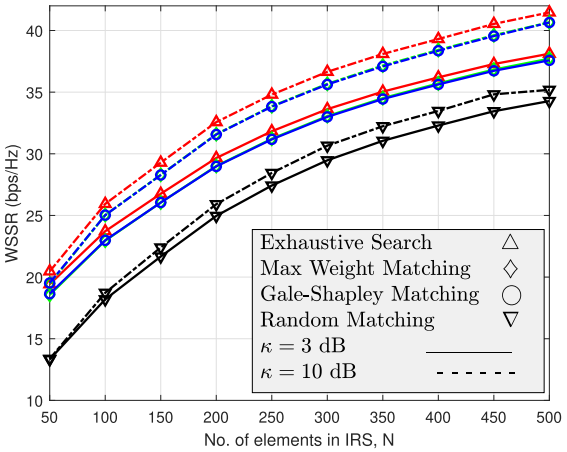

FIGURE 4. The WSSR performance versus the number of elements, N, in the IRS.

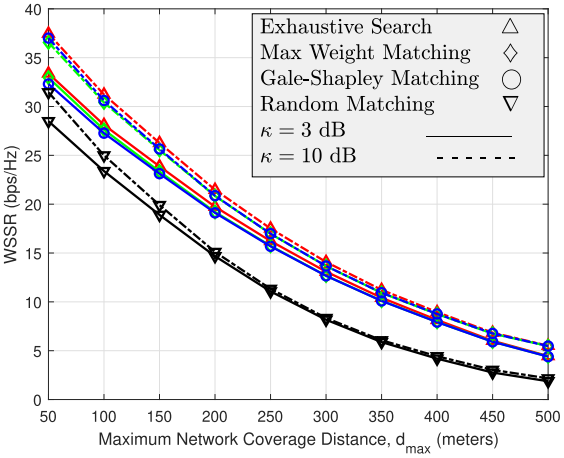

FIGURE 6. The WSSR performance versus the maximum network coverage distance, $d_{\max}$.

seen that the Gale-Shapley and maximum weight matching algorithms have similar WSSR performance. Furthermore, both the schemes perform close to the exhaustive search method. The effect of increasing the number of elements in the IRS on the WSSR is also evident in Fig. 4. This suggests that overall network security can be improved by increasing the number of IRS elements in the IRS (i.e., large N values). However, the WSSR performance increasing trend seems to slowly fade as the number of elements becomes too large. It can be seen from the figure, that if the number of elements in the IRS are increased 10 times, the WSSR performance or security of the network will be doubled.

The WSSR performance of the network is plotted in Fig. 5 against the number of transmit antennas, M. It is noticed that as the number of antennas at the transmitter is increased, the WSSR performance also improves gradually for all the plotted schemes. This improvement is due to the fact that the large number of antennas at the transmitter will result in efficient beamforming towards the Bob, while reducing any signal leakage towards the Eve. In Fig. 6, we vary the maximum distance, $d_{\max}$, between the transmitter and Bobs, and record its effect on the WSSR performance of the network. It can be seen that as the value of $d_{\max}$ increases, WSSR decreases. The reason for this decrease is the higher path loss values at large distances, which in turn decreases the WSSR performance.

VII. CONCLUSION

Smart and connected machines empowered by 5G technology can enhance the level of automation and monitoring of various processes in the industry. This network of machines, sensors and computing servers known as IIoT will significantly improve the industrial productivity. In this paper, we propose a PLS scheme that uses omni-IRS to improve the WSSR performance. We solve the problem of designing active and passive beamforming vectors by using AO technique, such that WSSR of the network is maximized. Furthermore, we provide a stable solution for omni-IRS selection using Gale-Shapley stable matching algorithm. We evaluate the performance of the proposed scheme using detailed simulations, and show that it can enhance the WSSR performance of machines by 40% as compared to random matching. The

minimum secrecy rate achieved through the Gale-Shapley algorithm is superior than the one achieved via maximum weight matching. Through simulations, we also observed that PLS of the outdoor IIoT can be improved by increasing the number of passive elements in the omni-IRSs, i.e., to use large size IRSs.

REFERENCES

[1] B. V. Natesha and R. M. R. Guddeti, "Fog-based intelligent machine malfunction monitoring system for industry 4.0," *IEEE Trans. Ind. Informat.*, vol. 17, no. 12, pp. 7923–7932, Dec. 2021.
[2] W. Ejaz, M. Naeem, and S. Zeadally, "On-demand sensing and wireless power transfer for self-sustainable industrial Internet of Things networks," *IEEE Trans. Ind. Informat.*, vol. 17, no. 10, pp. 7075–7084, Oct. 2021.
[3] W. Zhang, D. Yang, H. Peng, W. Wu, W. Quan, H. Zhang, and X. Shen, "Deep reinforcement learning based resource management for DNN inference in industrial IoT," *IEEE Trans. Veh. Technol.*, vol. 70, no. 8, pp. 7605–7618, Aug. 2021.
[4] B. Jiang, J. Li, G. Yue, and H. Song, "Differential privacy for industrial Internet of Things: Opportunities, applications, and challenges," *IEEE Internet Things J.*, vol. 8, no. 13, pp. 10430–10451, Jul. 2021.
[5] Y. Zhang and H.-Y. Wei, "Risk-aware cloud-edge computing framework for delay-sensitive industrial IoTs," *IEEE Trans. Netw. Service Manage.*, vol. 18, no. 3, pp. 2659–2671, Sep. 2021.
[6] W. Mao, Z. Zhao, Z. Chang, G. Min, and W. Gao, "Energy-efficient industrial Internet of Things: Overview and open issues," *IEEE Trans. Ind. Informat.*, vol. 17, no. 11, pp. 7225–7237, Nov. 2021.
[7] U. M. Malik, M. A. Javed, S. Zeadally, and S. U. Islam, "Energy-efficient fog computing for 6G-enabled massive IoT: Recent trends and future opportunities," *IEEE Internet Things J.*, vol. 9, no. 16, pp. 14572–14594, Aug. 2022.
[8] S. Qi, Y. Lu, Y. Zheng, Y. Li, and X. Chen, "Cpds: Enabling compressed and private data sharing for industrial Internet of Things over blockchain," *IEEE Trans. Ind. Informat.*, vol. 17, no. 4, pp. 2376–2387, Apr. 2021.
[9] H. Lin, J. Hu, X. Wang, M. F. Alhamid, and M. J. Piran, "Toward secure data fusion in industrial IoT using transfer learning," *IEEE Trans. Ind. Informat.*, vol. 17, no. 10, pp. 7114–7122, Oct. 2021.
[10] X. Wang, S. Garg, H. Lin, M. J. Piran, J. Hu, and M. S. Hossain, "Enabling secure authentication in industrial IoT with transfer learning empowered blockchain," *IEEE Trans. Ind. Informat.*, vol. 17, no. 11, pp. 7725–7733, Nov. 2021.
[11] M. Agiwal, A. Roy, and N. Saxena, "Next generation 5G wireless networks: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 3, pp. 1617–1655, 3rd Quart., 2016.
[12] Z. Lv, Y. Han, A. K. Singh, G. Manogaran, and H. Lv, "Trustworthiness in industrial IoT systems based on artificial intelligence," *IEEE Trans. Ind. Informat.*, vol. 17, no. 2, pp. 1496–1504, Feb. 2021.
[13] F. Al-Turjman and B. D. Deebak, "Seamless authentication: For IoT-big data technologies in smart industrial application systems," *IEEE Trans. Ind. Informat.*, vol. 17, no. 4, pp. 2919–2927, Apr. 2021.
[14] R. Taheri, M. Shojafar, M. Alazab, and R. Tafazolli, "Fed-IIoT: A robust federated malware detection architecture in industrial IoT," *IEEE Trans. Ind. Informat.*, vol. 17, no. 12, pp. 8442–8452, Dec. 2021.
[15] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1550–1573, 3rd Quart., 2014.
[16] H. Luo, Q. Li, L. Yang, and J. Qin, "An efficient algorithm for robust fractional QCQP and its applications to multiuser beamforming with bounded channel uncertainties," *IEEE Trans. Signal Process.*, vol. 70, pp. 6096–6111, 2022.
[17] M. A. Javed, E. B. Hamida, A. Al-Fuqaha, and B. Bhargava, "Adaptive security for intelligent transport system applications," *IEEE Intell. Transp. Syst. Mag.*, vol. 10, no. 2, pp. 110–120, Summer 2018.
[18] S. Kisseleff, S. Chatzinotas, and B. Ottersten, "Reconfigurable intelligent surfaces in challenging environments: Underwater, underground, industrial and disaster," *IEEE Access*, vol. 9, pp. 150214–150233, 2021.
[19] Y.-C. Liang, R. Long, Q. Zhang, J. Chen, H. V. Cheng, and H. Guo, "Large intelligent surface/antennas (LISA): Making reflective radios smart," *J. Commun. Inf. Netw.*, vol. 4, no. 2, pp. 40–50, Jun. 2019.
[20] D. Xu, K. Yu, and J. A. Ritcey, "Cross-layer device authentication with quantum encryption for 5G enabled IIoT in industry 4.0," *IEEE Trans. Ind. Informat.*, vol. 18, no. 9, pp. 6368–6378, Sep. 2022.
[21] S. Zhang, H. Zhang, B. Di, Y. Tan, M. Di Renzo, Z. Han, H. Vincent Poor, and L. Song, "Intelligent omni-surfaces: Ubiquitous wireless transmission by reflective-refractive metasurfaces," *IEEE Trans. Wireless Commun.*, vol. 21, no. 1, pp. 219–233, Jan. 2022.
[22] J. Xu, Y. Liu, X. Mu, and O. A. Dobre, "STAR-RISs: Simultaneous transmitting and reflecting reconfigurable intelligent surfaces," *IEEE Commun. Lett.*, vol. 25, no. 9, pp. 3134–3138, Sep. 2021.
[23] Z. Gu, H. Chen, P. Xu, Y. Li, and B. Vucetic, "Physical layer authentication for non-coherent massive SIMO-enabled industrial IoT communications," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 3722–3733, 2020.
[24] A. Jaiswal, S. Kumar, O. Kaiwartya, N. Kumar, H. Song, and J. Lloret, "Secrecy rate maximization in virtual-MIMO enabled SWIPT for 5G centric IoT applications," *IEEE Syst. J.*, vol. 15, no. 2, pp. 2810–2821, Jun. 2021.
[25] X. Yin, X. Fang, N. Zhang, P. Yang, X. Sha, and J. Qiu, "Online learning aided adaptive multiple attribute-based physical layer authentication in dynamic environments," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 2, pp. 1106–1116, Apr. 2021.
[26] Z. Zhang, C. Zhang, C. Jiang, F. Jia, J. Ge, and F. Gong, "Improving physical layer security for reconfigurable intelligent surface aided NOMA 6G networks," *IEEE Trans. Veh. Technol.*, vol. 70, no. 5, pp. 4451–4463, May 2021.
[27] H. Niu, Z. Chu, F. Zhou, and Z. Zhu, "Simultaneous transmission and reflection reconfigurable intelligent surface assisted secrecy MISO networks," *IEEE Commun. Lett.*, vol. 25, no. 11, pp. 3498–3502, Nov. 2021.
[28] J. Zhang, H. Du, Q. Sun, B. Ai, and D. W. K. Ng, "Physical layer security enhancement with reconfigurable intelligent surface-aided networks," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 3480–3495, 2021.
[29] S. Hong, C. Pan, H. Ren, K. Wang, and A. Nallanathan, "Artificial-noise-aided secure MIMO wireless communications via intelligent reflecting surface," *IEEE Trans. Commun.*, vol. 68, no. 12, pp. 7851–7866, Sep. 2020.
[30] J. Mirza and B. Ali, "Channel estimation method and phase shift design for reconfigurable intelligent surface assisted MIMO networks," *IEEE Trans. Cognit. Commun. Netw.*, vol. 7, no. 2, pp. 441–451, Jun. 2021.

BAKHTIAR ALI received the M.S. degree in personal and mobile radio communications from Lancaster University, U.K., in September 2008, and the Ph.D. degree in electrical engineering from COMSATS University Islamabad, Islamabad, Pakistan, in January 2018. His research interests include radio resource management in cooperative cognitive radio networks, reconfigurable intelligent surfaces, MIMO, cooperative communications, physical layer security, game theory, and the study of future radio communications systems, i.e., 6G.

JAWAD MIRZA (Senior Member, IEEE) received the B.Sc. degree in electrical (telecommunications) engineering from the COMSATS Institute of Information Technology, Islamabad, Pakistan, in 2007, the M.Sc. degree in communications engineering from The University of Manchester, Manchester, U.K., in 2009, and the Ph.D. degree from the Victoria University of Wellington, Wellington, New Zealand, in 2016. He was a Postdoctoral Research Associate with the Wolfson School of Mechanical, Electrical and Manufacturing Engineering, Loughborough University, U.K. He is currently an Assistant Professor with the Department of Electrical and Computer Engineering, COMSATS University Islamabad, Islamabad. His current research interests include intelligent reflecting surfaces aided multiple antenna communication systems, full-duplex transmission, and 6G wireless communication systems.

SAJID HUSSAIN ALVI received the M.Sc. and M.Phil. degrees in electronics from Quaid-i-Azam University, Islamabad, Pakistan, in 2001 and 2006, respectively, and the Ph.D. degree from the Department of Electrical Engineering, COMSATS University Islamabad (CUI) [formerly COMSATS Institute of Information Technology (CIIT)], Islamabad, in 2017. From 2004 to 2006, he worked as a Lecturer with the Department of Electrical Engineering, Air University, Islamabad. Since 2006, he has been working as a Faculty Member of CUI, where he is currently an Assistant Professor with the Department of Physics. His research interests include cooperative communications, terrestrial and aerial heterogeneous networks, and signal processing.

MOHAMMAD ZUBAIR KHAN received the M.C.A. degree in computer science and information technology, the M.Tech. degree in computer science, and the Ph.D. degree in computer science and information technology. He has worked as the Head and an Associate Professor with the Department of Computer Science and Engineering, Invertis University, Bareilly, India. He is currently a Full Professor with the Department of Computer Science and Information, Taibah University, Madinah, Saudi Arabia. He has three research grants from the Ministry of Higher Education, Government of Saudi Arabia. He has guided many students on the IoT, parallel computing, data mining, and machine learning. He has guided many students on the IoT, parallel computing, data mining, and machine learning. He has published more than 100 articles, including 45 articles in high-impact journals, and edited one book. He has been actively involved in research for building hi-tech systems to handle key challenges related to the Internet of Things, communication, machine learning, cyber security, and parallel and distributed systems. He has been a member of the Computer Society of India, since 2004. He serves as a scientific evaluator, a member of experts in several panels and committees at various universities; a member of the Ph.D. Committee, and has been invited for keynote and invited lectures at international conferences. He serves as an editorial board member and a reviewer for many peer-reviewed international journals.

MUHAMMAD AWAIS JAVED (Senior Member, IEEE) received the B.Sc. degree in electrical engineering from the University of Engineering and Technology, Lahore, Pakistan, in August 2008, and the Ph.D. degree in electrical engineering from The University of Newcastle, Australia, in February 2015. From July 2015 to June 2016, he worked as a Postdoctoral Research Scientist with the Qatar Mobility Innovations Center (QMIC) on the SafeITS project. He is currently working as an Assistant Professor with COMSATS University Islamabad, Pakistan. His research interests include intelligent transport systems, vehicular networks, protocol design for emerging wireless technologies, and the Internet of Things.

ABDULFATTAH NOORWALI received the Ph.D. degree in electrical and computer engineering from the University of Western Ontario, London, ON, Canada, in 2017. He is currently an Associate Professor with the Electrical Engineering Department, Faculty of Engineering and Islamic Architecture, UmmAl-Qura University. He has authored many technical papers in journals and international conferences. His research interests include smart grid communications, cooperative communications, wireless networks, the Internet of Things, crowd management applications, machines learning, computer networking, and smart city solutions.