IEEE Open Journal of
Vehicular Technology

Received 7 June 2022; accepted 13 June 2022. Date of publication 15 June 2022;
date of current version 12 July 2022. The review of this article was coordinated by Editor Jemin Lee.

Digital Object Identifier 10.1109/OJVT.2022.3183218

Towards a Unified Framework for Physical Layer Security in 5G and Beyond Networks

MUHAMMAD SOHAIB J. SOLAIJA (Student Member, IEEE), HANADI SALMAN (Student Member, IEEE), AND HÜSEYIN ARSLAN (Fellow, IEEE)

(Invited Paper)

Department of Electrical and Electronics Engineering, Istanbul Medipol University, 34810 Istanbul, Turkey

CORRESPONDING AUTHOR: MUHAMMAD SOHAIB J. SOLAIJA (e-mail: solaija@ieee.org).

This work was supported by the Scientific and Technological Research Council of Turkey (TUBITAK) under Grant 120C142.

ABSTRACT Wireless systems have become an increasingly pivotal part of our lives. Various critical applications and use cases such as healthcare, financial transactions, e-commerce, transportation, industrial automation, etc. rely on secure and reliable communication for their proper operation. Despite their widespread adoption, conventional cryptographic security mechanisms are unable to scale with the increasingly decentralized and heterogeneous networks. Physical layer security (PLS), on the other hand, provides a promising complementary solution to ensure authenticity, confidentiality, integrity, and availability of legitimate transmissions by exploiting the dynamic characteristics of the wireless environment. Despite the plethora of literary works regarding different facets of PLS being present, a unified framework is still absent. In this paper, we provide a PLS framework that not only encompasses the existing works but also enables the development of next-generation PLS methods. In line with this, the importance of PLS for emerging technologies such as joint sensing and communication, vehicular communication, non-terrestrial networks, millimeter-wave, terahertz communication, etc. is highlighted. Furthermore, the key challenges and directions for future PLS mechanisms are identified.

INDEX TERMS Artificial noise, authentication, availability, beamforming, channel, confidentiality, cooperative transmission, eavesdropping, integrity, jamming, physical layer security, PLS, radio environment, sensing, signal, spoofing, wireless security.

LIST OF ACRONYMS

1G	first generation.
3GPP	3rd Generation Partnership Project.
4G	fourth generation.
5G	fifth generation.
6G	sixth generation.
AI	artificial intelligence.
AoA	angle of arrival.
AP	access point.
APP	application.
ARQ	automatic repeat request.
BS	base station.
CBRS	Citizens Broadband Radio Service.
CFO	carrier frequency offset.
CFR	channel frequency response.
CIR	channel impulse response.
CLT	central limit theorem.
CoMP	coordinated multipoint.
CP	cyclic prefix.
CSI	channel state information.
D2D	device-to-device.
DL	deep learning.
DNN	deep neural network.
DoS	denial of service.
ELPC	extremely low-power communication.
eMBB	enhanced mobile broadband.
ERLLC	extremely reliable and low-latency communication.
FeMBB	further-enhanced mobile broadband.
FFT	fast Fourier transform.

FIR	finite impulse response.
FTR	fluctuating two ray.
HAPS	high altitude platform systems.
ICI	inter-carrier interference.
i.i.d.	independent and identically distributed.
IoT	Internet of things.
IP	Internet protocol.
IQI	in-phase/quadrature imbalance.
ISI	inter-symbol interference.
IT	information technology.
ITS	intelligent transportation system.
JSC	joint sensing and communication.
LDHMC	long-distance and high-mobility communication.
LDPC	low-density parity-check.
LED	light-emitting diodes.
LoS	line-of-sight.
LPI	low probability of intercept.
LTE	long-term evolution.
MAC	medium access control.
MCC	mission-critical communication.
MEC	mobile edge computing.
MIMO	multiple-input multiple-output.
ML	machine learning.
mMIMO	massive multiple-input multiple-output.
mMTC	massive machine-type connectivity.
MPC	multipath component.
MRC	maximal-ratio combining.
mmWave	millimeter-wave.
MEC	mobile edge computing.
NFV	network function virtualization.
NLoS	non-line-of-sight.
NTN	non-terrestrial network.
NWDP	N-wave with diffuse power.
OFDM	orthogonal frequency division multiplexing.
PAPR	peak-to-average power ratio.
PEAC	phase enciphered Alamouti coding.
PHY	physical.
PLS	physical layer security.
QoE	quality of experience.
QoS	quality of service.
REM	radio environment map.
RF	radio frequency.
RIS	reconfigurable intelligent surface.
RSS	received signal strength.
RSSI	received signal strength indicator.
SIMO	single-input multiple-output.
SISO	single-input single-output.
SON	self-organizing network.
SNR	signal-to-noise ratio.
TDD	time-division duplexing.
TDoA	time difference of arrival.
THz	terahertz.
TN	terrestrial network.
TWDP	two-wave with diffuse power.
UAV	unmanned aerial vehicle.
umMTC	ultra-massive machine-type communication.
uRLLC	ultra-reliable low-latency communication.
V2I	vehicle-to-infrastructure.
V2N	vehicle-to-network.
V2P	vehicle-to-pedestrians.
V2V	vehicle-to-vehicle.
V2X	vehicle-to-everything.
VLC	visible light communication.
WSN	wireless sensor network.
XAI	explainable AI.
XR	extended reality.

I. INTRODUCTION

A. MOTIVATION AND BACKGROUND

Wireless networks have evolved to the point of unrecognizability over the last few decades. Consider the brick-like cellular phones of the first generation (1G) which cost a fortune but only provided half an hour of talk time, and compare it to an average smartphone in the fourth generation (4G) era which brings the power of the internet (and so much more) to the palm of our hands. While the initial generations of the cellular system focused on connecting people together, firstly via voice/text and later using emails and social media, it was not until the fifth generation (5G) that a paradigm shift towards machine connectivity became obvious [1]. The introduction of three main classes of services, namely enhanced mobile broadband (eMBB), massive machine-type connectivity (mMTC) and ultra-reliable low-latency communication (uRLLC) opens the door for a variety of applications - ranging from education to gaming, healthcare to banking, industrial automation to autonomous driving, and so on - to become a reality [2].

The aforementioned services have their distinct requirements. For instance, eMBB targets high data rates and better spectral efficiency; mMTC is aimed at increasing the device density and battery life; uRLLC is focused on improving the reliability while reducing the latency for mission-critical applications [3]. The sheer diversity of requirements necessitates a variety of enabling technologies as well. Accordingly, some of the critical enablers identified for 5G include millimeter-wave (mmWave) communication, small cells, massive multiple-input multiple-output (mMIMO), beamforming and network function virtualization (NFV) [4], [5]. Moreover, even though 5G does not provide a completely different physical (PHY) layer waveform (which is usually a distinguishing feature between the different generations), it introduces flexibility in the shape of numerologies [6]. The increased heterogeneity of the network - in terms of device capability, network topology, frequency bands, numerology, application/user requirements - means that compared to the previous generations, 5G networks have to optimize an exceedingly large number of parameters [7]. Given the huge number of scenarios that may crop up and the possible decisions to take from a network's perspective, the shift towards the incorporation of artificial intelligence (AI)/machine learning (ML) has become inevitable [8]. With sixth generation (6G), the diversity of applications is going to

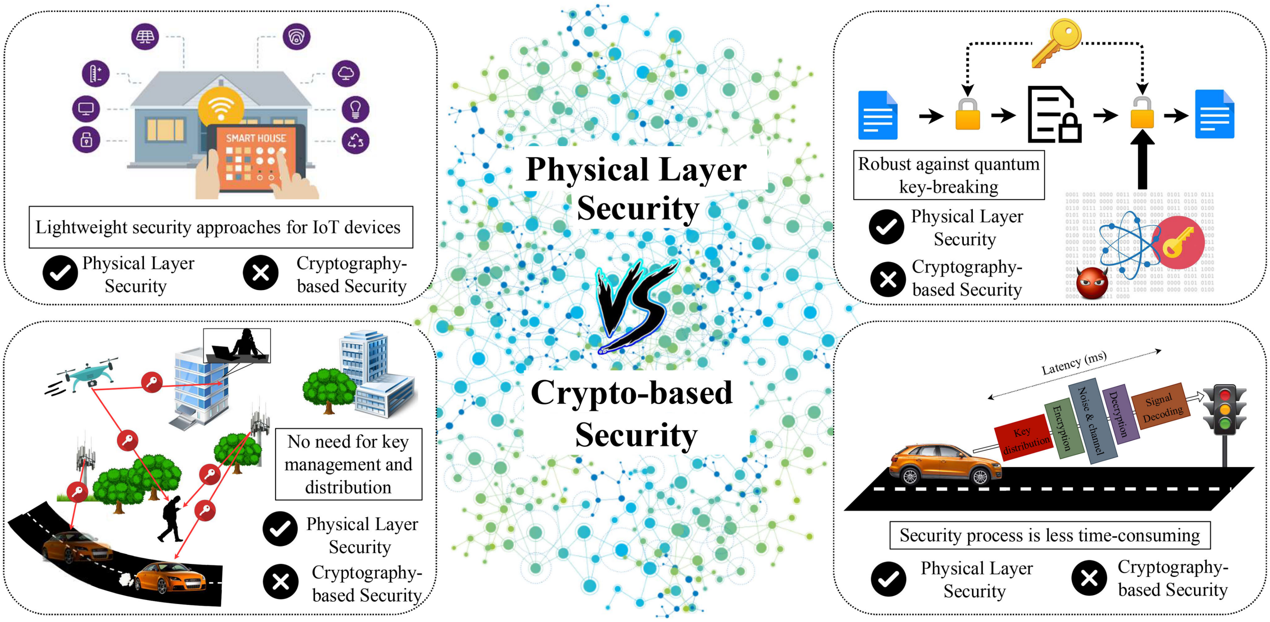

SMART HOUSE
Lightweight security approaches for IoT devices
✓ Physical Layer Security
✗ Cryptography-based Security
Physical Layer Security
VS
Crypto-based Security
Robust against quantum key-breaking
✓ Physical Layer Security
✗ Cryptography-based Security
No need for key management and distribution
✓ Physical Layer Security
✗ Cryptography-based Security
Latency (ms)
Key distribution
Encryption
Noise & channel
Decryption
Signal Decoding
Security process is less time-consuming
✓ Physical Layer Security
✗ Cryptography-based Security

FIGURE 1. Illustration of some wireless scenarios where conventional cryptography-based security struggles.

increase further with the services like further-enhanced mobile broadband (FeMBB), extremely reliable and low-latency communication (ERLLC), long-distance and high-mobility communication (LDHMC), ultra-massive machine-type communication (umMTC), and extremely low-power communication (ELPC) [9], [10]. The network optimization will, consequently, become even more complicated. Accordingly, various academic works regarding the 6G vision put AI/ML at the center of network design [11]–[13].

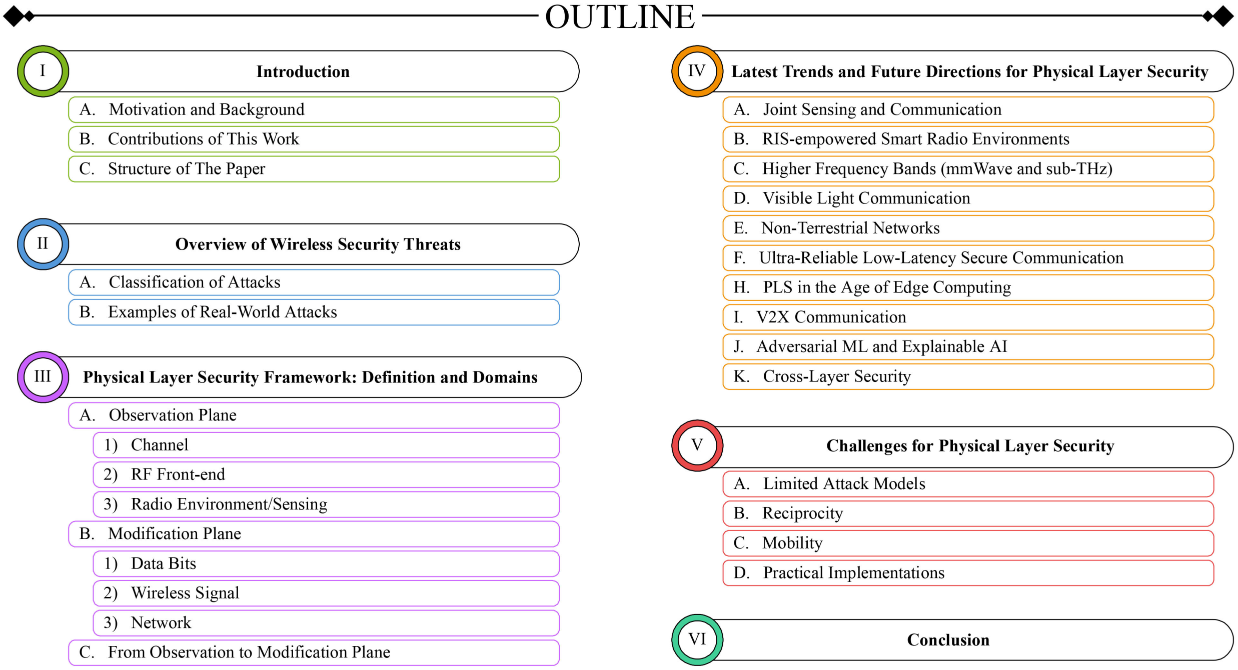
AI/ML, despite its promise, comes with certain potential vulnerabilities. As [14] points out, the increased use of AI leads to an expansion of the potential attack "surface". The next generation of wireless networks will generate even more data, and constraints such as limited capabilities of devices, increased heterogeneity of the network, and the dynamically changing wireless topology will further solidify the need for advanced security techniques [15]. The conventional security paradigm, i.e., *cryptography* does not scale well enough to address the diversity in applications, devices, and network deployment scenarios. As illustrated in Fig. 1, this is due to the following reasons: firstly, cryptographic security depends on the computational complexity of the key-breaking which is rendered a naive assumption with the advent of quantum computing [16]; secondly, in applications such as Internet of things (IoT)/mMTC the terminal devices are constrained in terms of power and other computational resources necessitating simple and lightweight security mechanisms [17]; thirdly, the high-mobility applications such as high-speed trains, vehicle-to-everything (V2X) communications and non-terrestrial networks (NTNs) manifesting in a continuously changing network topology require renewed key management and authentication procedures [18]; and lastly, for uRLLC/ERLLC applications, latency is a critical issue and conventional cryptographic methods might be too time-consuming to be practical [19]. The next-generation network, therefore, necessitates a new approach that could complement (if not replace) cryptography. Physical layer security (PLS) is arguably the most compelling candidate; it addresses the quantum threat by providing various alternatives where the security is ensured by providing better link quality for legitimate nodes compared to the illegitimate links [20]; unlike cryptography, which requires computational capabilities at both computing nodes, PLS also supports *asymmetrical* security mechanisms where the processing may be kept on the base station (BS)/access point (AP) side, rendering it suitable for IoT terminals [21]; PLS also simplifies the key management by allowing communicating nodes to extract keys from the channel observed between themselves, eliminating the need for secure key exchange [22]; moreover, since key exchange and encryption/decryption are not necessary, PLS boasts reduced latency compared to cryptographic approaches [23].

B. CONTRIBUTIONS OF THIS WORK

As evident from the above discussion, PLS is not necessarily a new topic. In fact, there is a plethora of academic works[1] that look at the different facets of PLS ranging from information-theoretic foundations to its practical implementation. That said, till now there is no unanimous definition for PLS or an accompanying framework that encompasses the different approaches developed. Accordingly, in this work we contribute the following to the PLS literature:

- Keeping in view the myriads of mission-critical applications expected in 5G and beyond networks, wireless

[1] Readers are referred to https://www.comsoc.org/publications/best-readings/physical-layer-security for a list of selected readings on PLS.


OUTLINE

I Introduction
A. Motivation and Background
B. Contributions of This Work
C. Structure of The Paper

II Overview of Wireless Security Threats
A. Classification of Attacks
B. Examples of Real-World Attacks

III Physical Layer Security Framework: Definition and Domains
A. Observation Plane
1) Channel
2) RF Front-end
3) Radio Environment/Sensing
B. Modification Plane
1) Data Bits
2) Wireless Signal
3) Network
C. From Observation to Modification Plane

IV Latest Trends and Future Directions for Physical Layer Security
A. Joint Sensing and Communication
B. RIS-empowered Smart Radio Environments
C. Higher Frequency Bands (mmWave and sub-THz)
D. Visible Light Communication
E. Non-Terrestrial Networks
F. Ultra-Reliable Low-Latency Secure Communication
H. PLS in the Age of Edge Computing
I. V2X Communication
J. Adversarial ML and Explainable AI
K. Cross-Layer Security

V Challenges for Physical Layer Security
A. Limited Attack Models
B. Reciprocity
C. Mobility
D. Practical Implementations

VI Conclusion

FIGURE 2. **Structure/outline of this paper.**

security is a non-negotiable requirement. Even though PLS has primarily been studied to secure communication, it applies to any wireless technology application including sensing. Accordingly, in this work, we provide a generalized framework for PLS that is relevant for all wireless systems.

- We split the PLS fabric into *observation* and *modification* planes and provide a novel manner of categorizing the existing (and future) PLS mechanisms depending on how they leverage the physical properties of the wireless signal and/or radio environment to secure the wireless link(s).
- The different *domains* of PLS are discussed under the modification and observation plane concepts, enabling a vision of future PLS mechanisms for next-generation wireless systems.
- The importance of PLS in paradigms such as NTNs, uRLLC, IoT, V2X, terahertz (THz), and joint sensing and communication (JSC) is highlighted, followed by identification of the associated technical challenges.

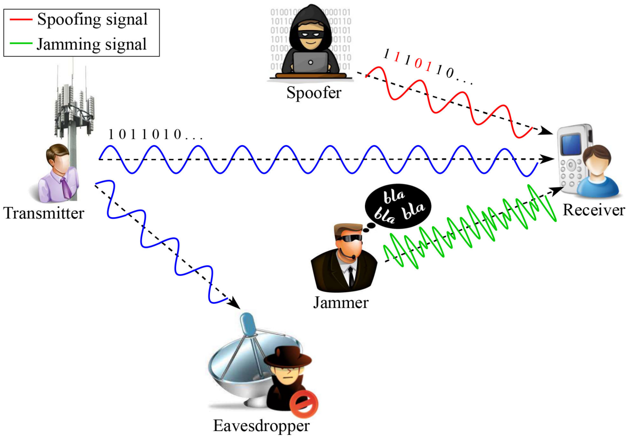


FIGURE 3. **Types of PLS threats in wireless network.**

C. STRUCTURE OF THE PAPER

As illustrated in Fig. 2, this article is structured in the following manner. Section II describes the wireless security threats with their associated motivations. Next, the proposed PLS framework is presented in Section III where its different domains are highlighted. Section IV sheds light on the importance of PLS in the latest technologies such as NTN, JSC, mobile edge computing (MEC), uRLLC, and IoT. The various challenges that need to be faced in realizing PLS along with future directions are discussed in Section V. Finally, Section VI concludes this work.

II. OVERVIEW OF WIRELESS SECURITY THREATS

Wireless systems enjoy a uniquely important place in our daily lives. While their ubiquitous presence simplifies countless tasks, the broadcast nature of wireless transmissions poses inherent security risks, some of which are illustrated in Fig. 3. In this section, we briefly describe the primary motivations behind various attacks before providing some examples from real networks.

A. CLASSIFICATION OF ATTACKS

The preliminary goal of PLS approaches is to make use of the properties of the PHY layer such as randomness of wireless channel and uniqueness of radio frequency (RF) fingerprints to address all the security requirements in wireless systems. These requirements are represented by the CIAA quartet (confidentiality, integrity, authenticity, and availability), fulfillment of which characterizes a secure and reliable communication system. In the following text, we will look at each requirement one by one along with the possible attacks that target them.

Confidentiality is arguably the first requirement that pops into one's head when thinking about communication security. A confidential system aims to limit the disclosure of information only to the legitimate receiver while preventing its interception by malicious entities [24]. The violation of confidentiality, referred to as an *eavesdropping* attack, results in the attacker being able to obtain and decode the secret data/signal content [20]. Conventionally, data encryption is the most commonly used technique for masking important and sensitive contents (where the encryption key may be shared or extracted from the wireless channel). In this case, an eavesdropper might be able to intercept the transmitted signal but cannot obtain any critical information from it [25].

Authentication ensures correct identification of the communicating nodes while integrity ensures that the message/data is not tampered with by the malicious attacker(s). A *spoofer*, on the other hand, attempts message injection, false reporting, data modification, and so on. A man-in-the-middle attack, for instance, is an attack against the integrity of information where, as the name implies, the attacker sits between the communicating nodes and manipulates the transmitted data [26]. To mitigate any inconvenience of such kind, the communicating nodes first perform mutual authentication (i.e., initial handshake) before establishing a communication link for data transmission using unique identities such as medium access control (MAC) and Internet protocol (IP) addresses. This step is to confirm that the communication request comes from the authorized nodes, distinguishing them from other nodes. It is evident that authenticity and integrity can be fulfilled simultaneously. For the sake of node authentication at the PHY layer, hardware [27], channel [28], and tag-based authentication [29] methods are employed.

Even if the transmitted data is kept confidential and its integrity and node authenticity maintained, it is often useless unless the authorized nodes are capable of accessing a wireless network anytime and anywhere upon request. The violation of availability, referred to as denial of service (DoS), will result in the authorized nodes being unable to access the wireless network, which in turn results in an unsatisfactory user experience. More specifically, a malicious node may launch DoS attack at the PHY layer by generating interference signals for disrupting the desired communication, which is also known as a *jamming* attack. This type of attack is segregated into proactive and reactive attacks [30]. A proactive jamming attacker transmits a jamming signal irrespective of the legitimate data transmission. As opposed to the proactive jamming attack, the reactive jammer starts jamming only over non-idle channels. To mitigate these attacks and ensure availability, we can use redundant communication links that become available when the primary link has been disrupted. Spread spectrum techniques are also used to combat jamming attacks by spreading the signal's energy over time and frequency domains [31].

B. EXAMPLES OF REAL-WORLD ATTACKS

To enable better understanding for the readers, we provide some examples of security breaches in real-world communication systems. These attacks typically involve low-end IoT terminals normally seen in smart city paradigms such as smart homes, transportation, and grids. Here it should be reiterated that conventional cryptographic approaches are relatively complex and, therefore, ill-suited to such applications.

Intelligent transportation systems (ITSs) envision the integration of sensing, control, analysis, and communication technologies into travel infrastructure and transportation to improve mobility, comfort, safety, and efficiency. As such, they rely heavily on secure V2X communication to ensure their smooth operation. However, malicious adversaries can disrupt their safety functions by injecting false measurements to compromise the security of drivers and pedestrians. In the case of obstacle/object detection, the falsified data might result in drivers making incorrect and unsafe decisions leading to collisions[32]. When launched on a larger scale, these attacks can cause multiple accidents, delays, and traffic jams. If combined with any disaster, it could even hamper the movement and performance of disaster-relief teams, leading to increased casualties.

Besides, the smart grid, which is basically the next generation of power electric system, relies on robust communication networks to provide efficient, secure, and reliable power delivery. Thus, network security is of critical importance in the smart grid. A set of attacks on the smart grid is investigated in [33], ranging from direct load shifting to meter data manipulation. Specifically, at a smaller scale, the adversaries can control certain IoT devices, such as home appliances, in the smart grid and induce an abnormal working state in these devices, e.g., increasing the power consumption. In terms of large-scale attacks, aggressive adversaries can compromise many high-wattage IoT devices to manipulate the power demand in a larger smart grid. The work in [34] demonstrates a large-scale attack model on real-world grids, using a botnet to turn on and off a large number of IoT devices synchronously, resulting in massive power fluctuations with the potential to cause a large-scale blackout.

In addition to the active attacks described above, smart home appliances such as IP cameras, smart motion sensors, AI speakers, and other IoT devices tend to have access to significant amounts of personal data through various user accounts as well as real-time spatial or positional information, which may be the target of passive eavesdropping attacks. An adversary may learn a user's behavioral patterns as well as

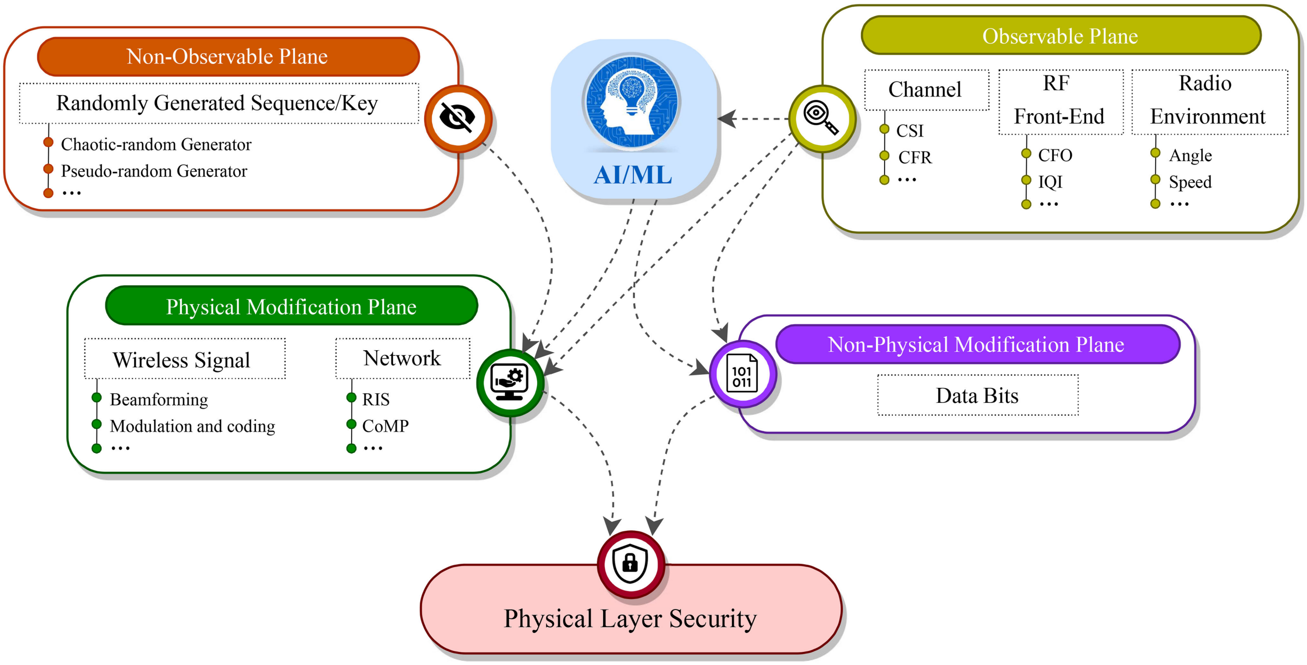


FIGURE 4. **Illustration of PLS conceptual framework.**

their credentials for different accounts. With such information, the adversary can then apply the password dictionary in a brute-force attack to guess the password and compromise the system. This has been demonstrated in a real-world case of IP camera identity leakage [35].

III. PHYSICAL LAYER SECURITY FRAMEWORK: DEFINITION AND DOMAINS

The basic idea of PLS is providing unbreakable, provable, and quantifiable secrecy from an information-theoretical point of view [24]. This is generally thought to be achieved through the intrinsic characteristics of the wireless channel such as fading, interference, and multipath propagation [36]–[38]. These methods are used to either authenticate the identity of the user or ensure confidentiality of the transmission by ensuring better signal reception at the legitimate receiver compared to the illegitimate/malicious attacker [39], [40]. Apart from the channel itself, other works have also exploited the hardware/RF properties of the transceivers for device authentication [41], as well as physical parameters (such as distance/angle between devices) in the environment to ensure confidentiality [42].

In essence, PLS admits the following approaches to its fold: (a) extraction of secret keys to encrypt/decrypt data bits, (b) modification of physical signal/transmission based on securely shared keys, and (c) modification of physical signal/transmission based on extracted keys. While the current literature boasts various works providing an overview of existing PLS techniques with the focus either on certain attack types or their counter-measures - such as [20], [43] focusing on confidentiality and [44], [45] targeting anti-jamming PLS mechanisms — a singular definition and framework that not only encompasses the existing works but also enables the development of next-generation PLS methods is still lacking. Consequently, in this work, we provide a PLS framework that plugs the aforementioned gap in the literature by elaborating how PLS is achieved by first observing and then utilizing the dynamic characteristics of wireless signals, RF front-end of the devices, transmission medium, and radio propagation environment to secure wireless transmissions[2].

Fig. 4 provides a high-level illustration of the PLS framework. Essentially, an observable plane serves as the source of randomness/uniqueness that can be leveraged to secure or authenticate wireless transmissions. These observations may come from the channel, RF front-end, or the radio environment as long as they follow certain criteria. The parameters extracted from the observation plane (or securely shared sequences) are then used to modify the transmissions on the bit, signal, or network level. However, it should be noted that in any approach either the observation or modification parameters should be physical in nature. For instance, the combination of non-observable shared sequence with bit-level modification is NOT considered to be covered under the PLS umbrella (rather it is considered to be cryptography). The following passage provides more details regarding the modification/observation planes with selected examples from the literature, while a summary of the same is provided in Table 1.

[2] Here we would like to clarify that the goal of this particular work is NOT to survey all PLS works, rather we just present selected works relevant to different categories of approaches to illustrate how they fit in with the proposed framework.

TABLE 1. Examples of Existing PLS Schemes Categorized According to PLS's Threats, Countermeasures and Definition

Threats	Countermeasures	Physical Modification	Observable Parameter	Example
Eavesdropping	Signal design	✓	✗	Constellation rotation using pseudo-random sequence [46], [47] and Chaotic-random sequence [48].
		✓	✓	Using channel information for constellation rotation [49], modulation selection [50], symbol interleaving [51], channel shortening filter design [52].
	Key generation	✗	✓	Generating channel-based key to secure the transmitted bits [53].
	Interfering signal	✓	✓	Design channel-based alignment signal [54].
		✓	✗	Adding pseudo-random artificial noise [55].
	Beamforming	✓	✓	Design channel-based linear precoding matrix [56].
	Cooperative communication	✓	✗	Utilizing cooperative jamming [57], [58], and CoMP [59].
Spoofing	RF/Hardware-based	✗	✓	Identify the receiver devices based on hardware features, e.g., IQI and power spectral density [60].
	Channel-based	✗	✓	Identify the receiver devices based on location features, e.g., RSSI and CSI [61], [62].
	Authentication tag	✓	✓	Generating channel-based authentication tags [63].
Jamming	Cooperative communication	✓	✗	Cooperative communication using trusted relays [64].
	Spread spectrum	✓	✓	Generating channel-based frequency hopping sequence [65].
		✓	✗	Utilizing pseudo-random frequency hopping sequence [31].
	Beamforming	✓	✗	Implementing directional antenna [66], and RIS [67]

A. OBSERVATION PLANE

The *observation* plane consists of the various parameters related to the wireless propagation environment that serves as a source of entropy and randomness which can be leveraged to secure the wireless link. These parameters should comply with the following properties:

- *Measurability:* This term indicates the extent to which the observable parameter is capable of being noticeable, visible, and discernible. Specifically, it must be quantifiable, i.e., it can be measured using a scientific process.
- *Reciprocity:* This expression implies that the observable parameter's response measured at location A is theoretically identical to the response measured at location B, considering that the wireless transmission takes place between location A and B.
- *Uniqueness:* For a particular transmission, the observable parameter should be unique, distinctive, and solitary in its characteristics. For instance, a third party that lies away from the legitimate transceivers should obtain a parameter uncorrelated to that between the legitimate parties.
- *Randomness:* From a statistics perspective, the observable parameter should have no apparent order and its individual values are uncertain and unpredictable. Specifically, the values of the observable parameter can be randomly modeled.

In the following text, we will evaluate the different domains, i.e., wireless channel, RF front-end, and radio environment, one by one in light of the same criteria.

1) CHANNEL

As a wireless signal passes through the propagation environment, the interaction between the signal and objects in the environment manifests in the form of phenomena such as absorption, reflection, refraction, and diffraction. These phenomena are rendered time-variant and random due to mobility in the environment [68]. From the communication perspective, the random behavior of the channel becomes challenging, especially in rich scattering environments since the coherence distance, time and bandwidth become limited. On the other hand, this is invaluable from the PLS perspective as the channel observations of legitimate and illegitimate nodes become independent (as long as they are half-wavelength apart).

Here it is important to look at the wireless channel in terms of the ideal properties of the observable plane parameters. Even though the interaction between the wireless signal and the environment is fairly complex, various models have been developed to provide a mathematical representation of the influence that the environment has on the signals. As such, various quantities such as received signal strength indicator (RSSI), channel state information (CSI), channel impulse response (CIR), and channel frequency response (CFR) are used to measure the channel. For the sake of modeling and analysis, the channel is generally represented as a finite impulse response (FIR) filter. If all other parameters (especially frequency) are kept constant, the channel is reciprocal, i.e., the channel response is the same in both uplink and downlink directions. In fact, reciprocity is one of the main motivations for the use of time-division duplexing (TDD) systems. Moreover, the propagation environment consists of several objects with different reflection/absorption capabilities, leading to multipath propagation, i.e., when different replicas of the signal arrive at the receiver with varying power levels and phases. These multipath components (MPCs) are modeled to be random and may add up constructively or destructively [69]. This randomness in turn means that the observed channel

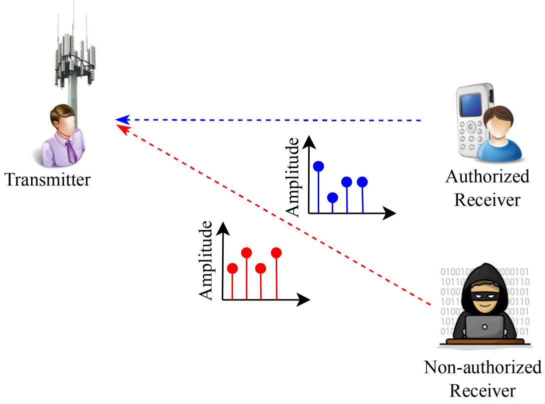


FIGURE 5. Difference in observed channel parameters such as CIR's amplitude (shown) and phase (not shown) can be used for link/device authentication.

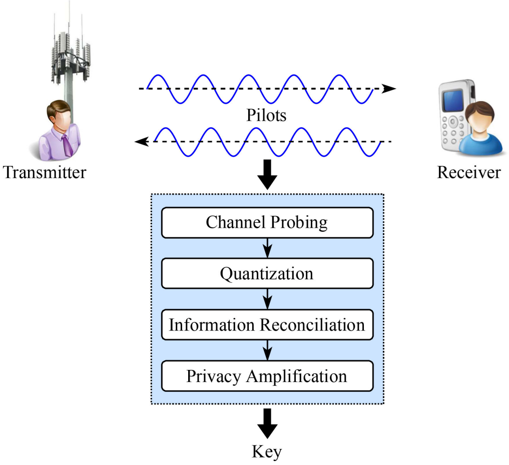


FIGURE 6. Basic steps for wireless channel-based key generation.

parameters are unique for different wireless links (as shown in Fig. 5), and can therefore be used for link authentication. For instance, in [70] an ML-assisted wireless fingerprinting approach is proposed to complement higher-level authentication where the identity of each node is validated by its wireless channel properties. It should be noted that the uniqueness of the channel depends on the richness of the environment which, in turn, is a function of transmission parameters like carrier frequency. In case the propagation environment has poor scattering, the assumption regarding the independence of legitimate and illegitimate channels may not hold [71]. Consequently, in such cases, it is advisable to complement channel-based PLS techniques with other approaches that consider RF front-end or radio environment map (REM) information, as discussed later.

One of the major advantages of exploiting wireless channel for PLS comes from the fact that channel estimation is an integral part of wireless communication. Since the wireless channel is highly dynamic, the communicating nodes need to know the effect that the environment has on the signal so that it can be removed, and a clean signal can be recovered at the receiver. The PLS methods, therefore, do not cause unnecessary overhead in terms of channel estimation. Consequently, wireless channel and its properties have been widely used in PLS for link adaptation [72], channel-based key generation [73], node authentication [74], and interfering signal injection [75].

In link adaptation, the goal is to utilize the independence of channel fading experienced by the legitimate and illegitimate nodes. In this category of approaches, the transmission parameters are adapted to optimize the communication over the legitimate link. Since the transmitted signal is adapted and optimized specifically for the legitimate receiver, it provides inherent security against any other user without requiring any additional processing or computation at the former [20]. Examples of link adaptation-based PLS approaches include subcarrier allocation [51], adaptive modulation and coding [72], power allocation [76], pre/post-coding [77], etc. As illustrated in Fig. 6, key generation has four main steps. The first step is called channel probing where both users obtain their measurements of the shared channel. This is followed by quantization, where the analog measurements are converted to binary values. The quantization level is usually dictated by the signal-to-noise ratio (SNR) level of the measured channel. Quantization is followed by the information reconciliation step to take care of any disagreement/mismatch in the earlier measurements. Since this step involves the public exchange of information between the legitimate nodes, it is possible a malicious node might also extract some information. Therefore, to ensure the security of the generated key, privacy amplification is employed where any compromised information/bits from the keys are removed [78]. In node authentication, the spatial decorrelation of the wireless channel between legitimate and illegitimate nodes is exploited to verify the identity of the user. Generally, node authentication consists of training and message transmission phases. In the former, a database of the channel fingerprint is built, while in the latter the actual transmission is tested against the database to corroborate that the current and prior transmissions are carried out by the same user [79]. Here, it should be noted that for channel-based authentication to be useful, both training and transmission phases need to occur within the coherence time of the channel. Interfering signal injection (discussed in detail in Section III-B2) includes techniques where intelligently designed signals are added on top of the transmitted data while taking into consideration the legitimate channel to ensure that they do not interfere with the legitimate reception.

Here, it should be reiterated that the channel observations are in fact a function of the transmission parameters used. For instance, path loss depends on the carrier frequency, with higher frequencies such as mmWave and THz undergoing significantly increased attenuation compared to the conventional systems. Since the classical channel models were developed for sub-6 GHz bands, they are unable to capture the propagation at these higher bands. As [80] illustrates, non-line-of-sight (NLoS) environment can not be modeled by a Rayleigh distribution at 28 GHz while a similar observation for THz bands is provided in [81]. Given that propagation in mmWave and THz bands is similar to each other [82], while being vastly different from conventional systems, it is necessary to develop and utilize more appropriate (and accurate) models capable of representing the heterogeneous networks expected in beyond 5G networks. Consequently, based on two-wave with diffuse power (TWDP) model [83] - which provides a physical explanation of why Rayleigh/Rician fading might not completely capture wireless fading - other models such as N-wave with diffuse power (NWDP) [84] and fluctuating two ray (FTR) [85] have been developed. NWDP generalizes TWDP to include N dominant MPCs in addition to the diffused components. The impact of the number, amplitudes, and total power of these dominant MPCs on PLS metrics such as secrecy outage and capacity is provided in [84]. The authors analytically show that a more unbalanced distribution of amplitudes amongst the dominant MPCs of legitimate link compared to illegitimate one can significantly increase secrecy. The security analysis for FTR is found in [86], where the authors validate that increasing (decreasing) SNR of the legitimate (illegitimate) link leads to secure communication, and light shadowing in the eavesdropper's link improves secrecy capacity. In addition to the diffuse component-based models, other generalized models have also been proposed recently. κ-μ fading model, which provides a generalized representation of line-of-sight (LoS) environment, has been analyzed from secrecy capacity and secrecy outage probability in [87]–[90] where [88], [89], and [90] focus on single-input single-output (SISO), single-input multiple-output (SIMO) and multiple-input multiple-output (MIMO) systems, respectively. Secrecy outage for α-η-μ and α-κ-μ in presence of a passive eavesdropper is provided in [91]. It should be noted that α-η-μ model is used to represent the NLoS propagation with its non-linearity and non-homogeneous nature, while α-κ-μ models propagation where LoS link also exists. Secrecy capacity and outage analysis of the even more general α-η-κ-μ model, which has been shown to fit well with the measurements at mmWave frequencies [92], has been provided in [93]. (For more details regarding the performance of PLS methods under generalized fading models, readers are referred to [94]).

2) RF FRONT-END

In addition to the wireless medium itself, the RF front-end also suffers from imperfections leading to impairments such as clock jitter, phase noise, carrier frequency offset (CFO), in-phase/quadrature imbalance (IQI), non-linearity of the power amplifier, and antenna imperfections [95]. Since these impairments vary from device to device, they can be considered as device "fingerprints" that may then be used to distinguish between different devices [41]. As such, RF fingerprinting is one of the popular PHY layer authentication mechanisms (see Fig. 7), targeted at eliminating (or at least detecting) any attacks on the node identity or message integrity. Another benefit of using RF fingerprint is how they complement the channel-based authentication. This is illustrated in [96], where device authentication is carried out using the device fingerprint while channel-based key generation is applied for secure communication in IoT devices. In general, while the channel-based methods are considered to be more appropriate for indoor and relatively stationary environments (so that authentication is not needed too frequently), the RF-based approaches can be leveraged in mobile environments due to their stability.

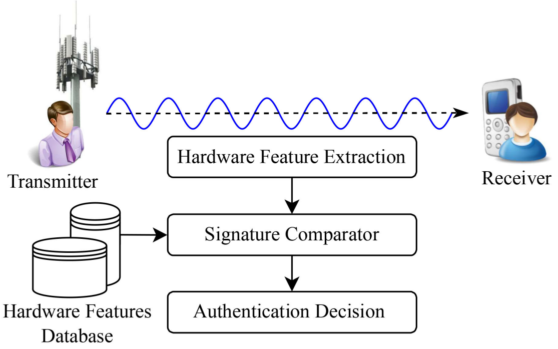


FIGURE 7. The RF impairments serve as potential "fingerprints" for wireless nodes.

One of the challenges faced in RF-based PLS, however, is the reliability of the fingerprint in real network conditions. For instance, a single impairment may not provide enough dynamic range to enable distinction between devices. Different approaches to address this have been studied with [97] using a weighted combination of multiple device characteristics, while [98] discusses a collaborative approach to where observations from multiple nodes are used to authenticate a device. Similar to channel-based PLS, a major motivation for using RF impairment-based security solutions is the fact that they need to be identified/measured anyway to ensure reliable communication. However, a major issue in this regard arises when the hardware impairments have a similar effect on the signal as certain channel-related phenomena. For instance, mobility in the environment leads to Doppler spread/shift which is, in essence, a change in the frequency as seen by the receiver. This is similar in effect to the local oscillator imperfection leading to CFO and imperfect frequency synchronization. In such scenarios, one approach might be to try and separate the channel effects from device impairments utilizing the fact that the former are varying on a much smaller time scale while the latter are more stable [99]. An alternative to this is to incorporate both the channel and RF-based impairments into a time-varying device fingerprint, as illustrated in [100], where the CFO due to oscillator mismatch is combined with channel induced Doppler into a time-varying CFO used for authentication of the device. A similar approach is used in [101], [102]. In the former, imperfect or "chaotic" antenna geometries and activation sequences are used for authentication while in the latter beamspace representation of the mutual coupling between multiple antennas of a mmWave MIMO system is used for the same purpose.

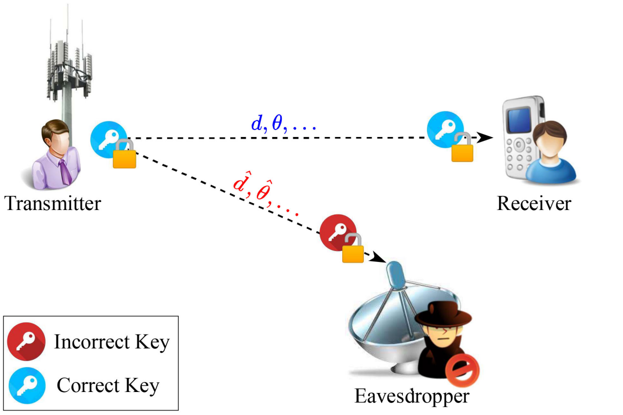


FIGURE 8. **The physical parameters observed from the environment (such as distance or angle between the nodes) serve as the source of keys to be used for PLS.**

3) RADIO ENVIRONMENT/SENSING

As wireless signal traverses the air, it experiences different phenomena (such as absorption, reflection, refraction, diffraction, etc.) due to the objects and their properties in the surrounding environment. Similar to the independence of the channel in a rich scattering environment, the surrounding objects and their properties might also be independent and therefore, serve as an environment fingerprint for different links. Properties such as distance, speed, angle, size of objects, or their constituent materials exemplify the different observable parameters that can be considered to either authenticate or secure a wireless link [103]. Figure 8 illustrates how different physical parameters can be used to generate keys in the network.

The most popularly used environment-related physical measurements for PLS include the distance or angle between the communicating nodes. For instance, the angle of arrival (AoA)-based key generation is employed in [104], where azimuth, elevation, or both angles are used to generate the secret key. The authors argue that AoA-based approach exhibits a lesser mismatch rate compared to channel-dependent key generation, rendering it more suitable for low SNR scenarios. Moreover, [42] proposes key generation based on the relative location of the communicating nodes. Since the relative location or distance is a reciprocal quantity, it eliminates the need for sharing the entropy source between the devices. There are various ways of calculating the distance, such as received signal strength (RSS) or time difference of arrival (TDoA)-based approaches [105]. As in the case of RF-based approaches mentioned earlier, it is possible to use parameters obtained from the radio environment or sensing in conjunction with channel knowledge, as is the case illustrated in [106]. It should be pointed out that in our generic PLS framework the sensing is not limited to RF domain. It is also possible to incorporate the information learned from external sensors including (but not limited to) cameras, LiDar, humidity/temperature sensors, etc.

B. MODIFICATION PLANE

In the previous subsection, we looked at the *observation* plane which serves as the source of randomness/entropy which can then be exploited to secure the wireless link. The exploitation can be realized on the bit, the signal, or the network domain, which collectively make up the *modification* plane.

1) DATA BITS

Wireless security mechanisms have conventionally been employed at the bit level. Classically, data is secured by converting the message or *plaintext* to *ciphertext* using some encryption mechanism [107]. Here it is important to make the distinction between cryptography and key-based PLS. In both cases, the transformation takes place at the bit level. In the former case, the key may or may not be shared between the communicating nodes in the cases of symmetric and asymmetric encryption, respectively. Either way, the encryption is done on the basis of a known/shared sequence. Since this process, including the key sharing/management, is generally carried at higher layers, it is not covered under the PLS paradigm. On the other hand, PLS incorporates the key-generation mechanisms depending on the observable parameters related to the wireless channel and the radio environment around the communicating nodes as discussed in the previous section. Since both transceivers observe the same channel/environment from which the key is extracted, there is no need for key exchange in PLS mechanisms [108]. In addition to key-based PLS, channel coding has also been utilized to provide security at the bit level. While various realizations of this exist (including polar [109], low-density parity-check (LDPC) [110] and other genres of codes [38]), one of the critical limitations of coding-based mechanisms is that the eavesdropper's (wiretap) channel needs to be degraded as compared to the legitimate link [111].

It should be noted that modification on the bit level is merely targeted at protection against eavesdropping. Jamming and spoofing are not addressed under this paradigm, which also happens to be a significant limitation of the standard cryptographic security solutions.

2) WIRELESS SIGNAL

The majority of the work pertaining to PLS arguably falls under the wireless signal domain. Here it should be noted that in the context of *modification* plane, wireless signal covers all the blocks between the coded bit-stream of data and the antenna at the transceivers. In the case of eavesdropping, this category of security solutions essentially aims to provide better data decoding capability at the legitimate receiver compared to the malicious attacker. This can either be done by intentionally degrading the performance of the eavesdropper or by improving the quality of service (QoS) for the legitimate receiver. Methods such as adaptive resource allocation [72] or **beamforming** [112] in the direction of legitimate node inherently provide some PLS since they are aimed at improving its link quality. Although the design of beamforming can be done according to different criteria (linear [113], [114] or nonlinear [115], [116]), a common goal is to direct the legitimate signal towards the legitimate receiver, while reducing the signal strength at the eavesdropper direction by making use of the spatial degree of freedom. A challenging issue in guaranteeing PLS arises if the eavesdropper is located closer to the transmitter than the legitimate receiver. In this context, the secrecy performance of spatial beamforming may not be satisfactory. On the other hand, there are various realizations where **the interfering signal** may be generated at the eavesdropper such that it lies in the null space of the legitimate receiver, i.e., it does not interfere with the legitimate receiver's signal. For this, certain works assume knowledge about eavesdropper location/CSI and modify signals such that decoding capability at that particular node is degraded. For instance, [117] and [118] assume knowledge of the eavesdropper's CSI while adding artificial noise to the transmitted signal. However, this assumption cannot be counted upon, especially in the case of passive eavesdroppers. The more realistic alternative is to design interfering signals just considering the legitimate link's information. This is evident in [119] where the legitimate transmitter only knows the legitimate channel and has fewer antennas than the eavesdropper. Similar to this, noise-loop modulation is proposed in [43] guaranteeing secure and reliable transmission. In this approach, the legitimate receiver purposely jams the transmission by deliberately introducing noise in the channel leading to the concealment of the information from the illegitimate node, no matter its computational power. Another PLS approach, called **signal design** [120], has shown significant performance gain in preventing reliable data transmission to eavesdroppers by altering the signal structure (e.g., modulation scheme, constellation structure, extra process, etc.) such that an eavesdropper is unable to decode the received signal correctly. Constellation adaptation depending on the legitimate CSI has been proposed in [121] where the constellation order (and mapping) is modified depending on the channel phase. As a result, the eavesdropper is unaware of the modulation scheme/order being used in the transmission block and therefore, incapable of demodulating it as shown in Fig. 9. In addition to channel-based sequences, other shared sequences have also been used for constellation rotation [46], [47]. All these approaches lead to a seemingly chaotic signal [48], characterized by a cloudy/distorted constellation, being observed by the eavesdropper. Channel-based shortening is proposed in [52] where a shortening filter is designed to reduce the effective delay spread at the receiver and the cyclic prefix (CP) is reduced accordingly leading to inter-symbol interference (ISI) at the eavesdropper. The authors in [122] propose adaptive and flexible PLS algorithms where data and pilots are jointly secured. Particularly, minimum-phase all-pass channel decomposition is exploited, where the proposed algorithms precode the data and pilots using the all-pass component of the channel which is random enough to provide security without causing peak-to-average power ratio (PAPR), thus not harming the performance of the legitimate user. Apart from the channel knowledge, RF impairments have also been used to secure communication. For instance, in [123] the authors leverage the CFO by pre-equalizing its combined effect with the channel to provide secure communication. Since CFO of the legitimate link is independent of and unknown to the eavesdropper, the eavesdropping quality is degraded.

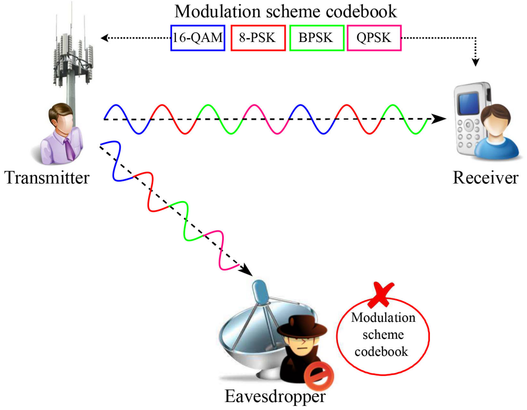


FIGURE 9. The modulation order/scheme is modified according to channel information making it difficult for the eavesdropper to intercept and demodulate the signal.

In terms of jamming, the most commonly utilized **spread spectrum** approach is to dynamically change the frequency at which the legitimate transmission is taking place to disrupt the jamming. The frequency hopping can be done on the basis of a pre-shared sequence [31], or alternatively, a channel-dependent sequence can be utilized [65]. While these approaches might be sufficient for rudimentary jamming attacks where the attacker does not have the capability to monitor and adapt to frequency hopping, more sophisticated and intelligent jammers capable of monitoring the transmission can still be problematic. To address such attacks, a rather interesting approach is developed in [124] where the legitimate transmitter leverages deep reinforcement learning to first understand the jammer's strategy and then find the optimum countermeasure. It adapts its own transmission parameters in addition to harvesting the energy from the jamming signal. This does not only waste the attacker's power resources but also enables the legitimate node to augment its own transmission via ambient backscatter communication.

As far as spoofing is concerned, most PLS solutions target the authentication of the communicating node (and thereby the message itself) using either the wireless channel [62] or RF impairments [60]. Neither of these approaches requires any modification of the transmitted signal. However, a handful of works have proposed the addition of an **authentication tag** to the wireless transmission. The tag, independent of the message, is encrypted and embedded into the transmitted signal and used to differentiate the legitimate device from an illegitimate one[125].

It is evident from the above discussion that a plethora of signal modification PLS solutions have been developed against eavesdropping. Moreover, modification of the signal parameters is arguably the only effective approach to mitigate jamming. On the other hand, signal modification is not necessarily the best (or most popular) approach for protection against spoofing.

3) NETWORK

The network in the context of the *modification* plane refers to the different nodes present in the environment. This may include relays in a cooperative communication scenario, BSs in a coordinated multipoint (CoMP) architecture and reconfigurable intelligent surfaces (RISs) in smart radio environments. The cooperative communication paradigm has gained increasing popularity since it enables otherwise resource-constrained devices to reap the diversity benefits of MIMO technology in a distributed manner with the help of helper nodes or relays [126]. The cooperative communication process usually has two phases, where the first phase involves the broadcast transmission from the source (to both relay and destination), while in the second phase the relay retransmits the signal towards the destination [127]. These systems are regularly deployed in ad hoc or wireless sensor networks (WSNs), where the decentralized structure, coupled with device limitations renders the authentication more burdensome compared to conventional cellular or Wi-Fi systems. The lack of authentication leads to the possibility of malicious attackers posing as relays to adversely affect the communication. Accordingly, several approaches relying on cooperative relaying and jamming have been developed to alleviate the issue of untrustable relays [128]. In cooperative relaying, if there is the possibility of eavesdropping, trustworthy relay(s) are selected to avoid interception of the message. However, this might inhibit the diversity benefit which is the primary motivation of cooperation. Alternatively, in cooperative jamming, a known jamming signal is transmitted by either source, destination, or a helper node to disrupt the potential eavesdropper's interception. In the case of destination-based jamming [129], while the need for a helper is eliminated, the system cannot take advantage of the diversity unless the destination has full duplexing capability. Moreover, jamming, in general, is a power-hungry approach. An interesting workaround to this problem is provided in [130] exploiting the properties of fast Fourier transform (FFT) operation in orthogonal frequency division multiplexing (OFDM) transmissions, where the destination node transmits a jamming signal only during the CP duration of the broadcast phase. The FFT operation causes this jamming signal to spread throughout all the subcarriers at the relay, causing inter-carrier interference (ICI) and reduced interception. Since the signal is only transmitted for a limited (i.e., CP) duration the proposed solution is more power-efficient and does not require full duplexing capability.

Unlike cooperative communication, CoMP is strictly a cellular concept developed to mitigate the inter-cell interference, particularly for small cells and heterogeneous network deployments. CoMP was initially introduced for long-term evolution (LTE) in 3rd Generation Partnership Project (3GPP) Rel-11 [131], with various enhancements in the succeeding releases. While it is not the primary driver behind CoMP, a handful of works have looked at CoMP from other perspectives including PLS [132]. In an underwater communication scenario, the transmissions from multiple distributed antenna elements are scheduled (and their power controlled) such that the received signal at the legitimate receiver is clean and non-overlapping (from the different antenna elements) while the packets from different antenna elements overlap and interfere at the eavesdropper [59], as shown in Fig. 10. The distributed BSs are also utilized to overcome the limitation of directional modulation where the eavesdropper lies in the same direction as the legitimate receiver [133]. This concept has also been extended to sparse environments, where coordination ensures that the transmitted message is only recoverable at the intersection of the transmissions from cooperating BSs [134]. The multipoint (or multi-landmark) is also extended to authentication, where RSSI observations are obtained at various physical locations to confirm the identity of a user [135]. The presence of multiple antennas at each landmark also provides better spatial resolution to further improve the accuracy of authentication.

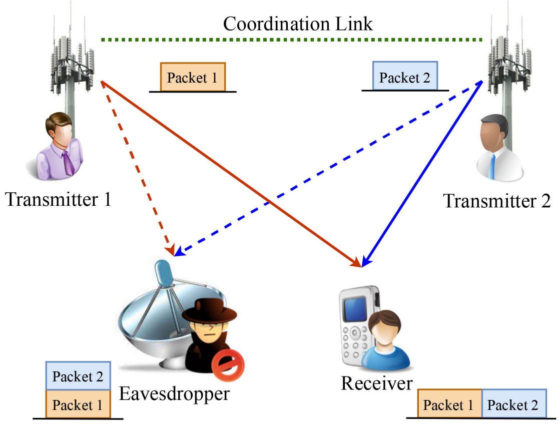


FIGURE 10. Intentional misalignment of the received packets (sent from different antenna elements) at eavesdropper to degrade its interception capability.

In conventional wireless systems, the propagation channel is a function of the surrounding radio environment. It is, therefore, assumed to be uncontrollable and the transceivers can only try to compensate/mitigate this effect. Given that information-theoretic PLS requires the legitimate user's channel to be better than the illegitimate one's, the uncontrollable nature of the channel can be a hindrance to ensuring the security of communication [136]. However, the smart radio environment paradigm empowered by RISs envisions wireless channel as a controllable entity [137], which opens various new avenues for PLS using RISs. The authors in [138] further explore RISs in beamspace context and show how the channel is converted from a design problem with unknown gains into a design element with controlled gains. Having a controlled object in the environment opens a new dimension in addressing current and future problems in the wireless network. For instance, the scatterers in RIS can be programmed to fast fade the channel of an eavesdropper, while maintaining a stable channel for intended users. Essentially, there are two main ways in which RISs can be exploited for secure communications, i.e., either by improving the secrecy rate/capacity of legitimate users or by enabling covert communications to hide the ongoing communication from the illegitimate user.

A survey of the former approaches is provided in [139], where various scenarios, systems models, optimization problems, and methodologies are discussed. RIS enables joint active/passive beamforming at the transmitter and RIS, respectively, using a large number of antenna elements available at the latter. This has been used to protect the communication from eavesdropping in [140], even in the presence of a stronger eavesdropper channel compared to the legitimate one in a LoS propagation environment. Joint beamforming is also discussed in [141], where authors motivate the use of RIS in mmWave and THz bands in the presence of a passive eavesdropper. RIS, in conjunction with artificial noise, is discussed in [142], where multiple eavesdroppers are present in the vicinity of the RIS. The impact of RIS on secrecy outage and average secrecy capacity in a vehicular paradigm is studied in [143], where the authors consider two scenarios, i.e., when the RIS is adjacent to the transmitter, and secondly when it is mounted on a building on the roadside. In [144], RIS is exploited to provide secure connectivity in device-to-device (D2D) scenario where the direct link between users is unavailable.

RISs have also been purported as enablers for covert communication. For instance, [145] considers the case where a *warden* tries to detect the communication while an eavesdropper aims to intercept it. In such a system (or adversary) model, not only is the secrecy capacity to be optimized but also the received power at the warden needs to be minimized. In [146], adversarial machine learning is employed for deep neural network (DNN)-empowered illegitimate receiver to ensure that the adversarial perturbations in transmissions have an adverse effect on its detection capability, while the legitimate receiver can still detect the communication successfully. An RIS-based transmitter is proposed in [147] for a JSC system to embed communication symbols in the radar waveform in a covert manner. A hybrid relay/RIS is proposed in [148] where a joint power allocation and relay/reflection coefficient selection problem is formulated to ensure reception of the transmission at the legitimate receiver while ensuring its covertness from the warden.

Additionally, RISs have been exploited in [67] to protect communication against jamming attacks. In particular, the joint optimization of beamforming and power allocation is studied with the goal of ensuring that the QoS requirements of the users are met in the presence of a multi-antenna jammer. Moreover, as mentioned earlier, from the PLS perspective a rich scattering channel is more desirable as it provides more randomness. One of the potential benefits of using RISs is controlling the variation in the channel over time, which can then be used for various purposes including PHY layer key generation [149].

The network-based PLS generally utilizes the macro-diversity to increase the reliability of a user's communication link while degrading the attacker's efficacy. These methods are primarily applicable to eavesdropping and jamming attacks, with limited effort to utilize cooperation in the networks for authenticating users.

C. FROM OBSERVATION TO MODIFICATION PLANE

As mentioned earlier, there are two primary components of the PLS framework discussed in this work. The first, i.e., the observation plane is the source of unique randomness that can be exploited by the second, i.e, modification plane to secure wireless transmissions. However, this raises the question about the decision mechanism that serves as the bridge between the aforementioned planes. In essence, what parameters should be observed in a given scenario, how long should they be observed, how should they be processed and analyzed, and consequently which approach in the modification plane should be utilized. Given that even for the same user, the security requirements may vary depending on the application being used, it is imperative that the system is capable of adapting in real-time. As such, the role of AI and self-organizing networks (SONs) becomes extremely critical. The original concept of adaptive or "cognitive" PLS was introduced in [150], further motivated in the context of V2X communication in [18], and finally a framework was provided in [151]. Like much of next-generation systems, optimized PLS is dependent on learning on the fly. The role of AI extends from signal analyses to modeling the behavioral characteristics of the users in the observation plane. The information about the environment is then utilized to identify any anomalies that exemplify the presence of malicious entities [99]. Following that, the appropriate selection of PLS mechanism, resource allocation, signal processing method, node selection (in network domain) needs to be carried out. However, it should be highlighted that AI itself suffers from various potential threats in the form of adversarial ML, and countermeasures must be taken to mitigate them [152].

IV. LATEST TRENDS AND FUTURE DIRECTIONS FOR PHYSICAL LAYER SECURITY

Starting from 5G, each generation of wireless networks is expected to further diversify its use cases and applications. As a result, new technological paradigms are also expected to arise. In this section, we look at some 5G and beyond archetypes (shown in Fig. 11) from a PLS perspective.

A. JOINT SENSING AND COMMUNICATION

Sensing (radar) and communication are two of the foremost wireless technologies that have developed independently for decades. However, with the increase in the number of devices and applications for both, as well as the mutual reliance, there has been a push towards JSC in recent years. This is primarily

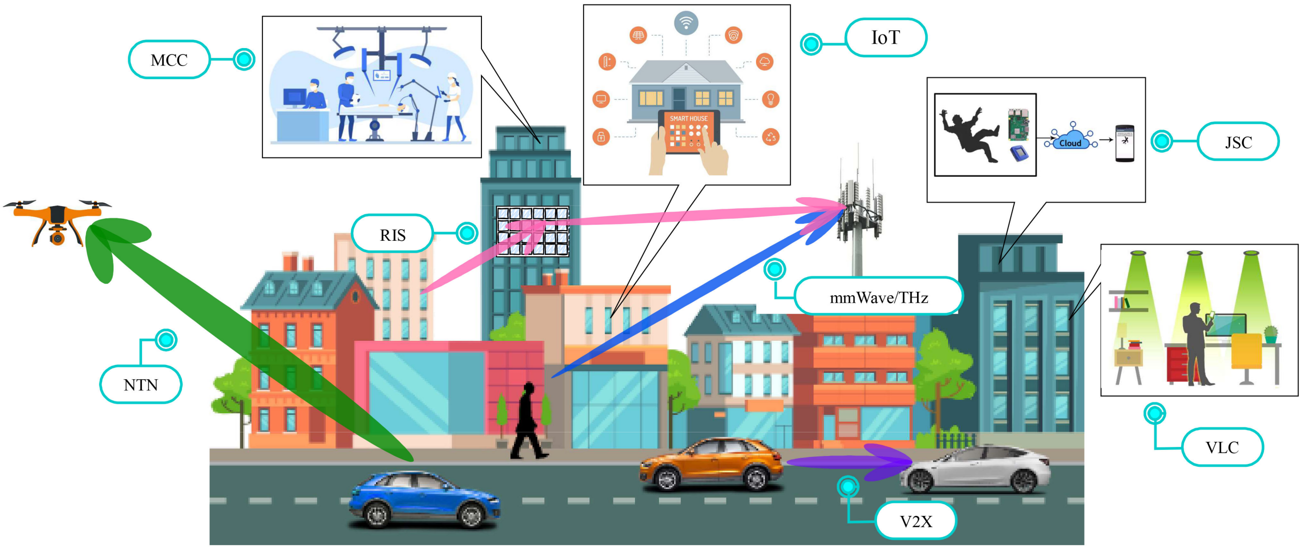


FIGURE 11. **An illustration of the emerging technological trends for beyond 5G network paradigms where PLS might prove critical.**

driven by spectrum scarcity, power limitations, and general similarities in the hardware. The joint design, however, has certain drawbacks as it leads to degradation in performance of either communication or sensing compared to the conventionally stand-alone systems [153]. Since sensing involves the transceivers acquiring information about their targets using wireless transmissions and their reflections [154], it raises serious concerns about user privacy and its vulnerability to any malicious nodes in the surrounding. In [151], the authors present a framework for JSC radio environment security in addition to exploring the suitability of existing PLS methods for sensing. For sensing, the attacks might target the sensing process, nodes, or the environment. In a process-oriented attack, the main goal is to manipulate the wireless sensing process. Low probability of intercept (LPI)-based [155] and randomized probing-based [156] solutions are used, for instance, to defend against spoofing attacks on sensing system. Node-oriented attack targets the different nodes that are part of the radio environment awareness and mapping process. These nodes may support communication, sensing, or both. The attacker might be interested in information such as node's identity, data, velocity, angle, location, RF characteristics, power, and waveform used [157]. The environment-oriented attacks are on the physical-radio environment. This includes changing the LoS/NLoS characteristics, channel richness and sparsity, urban/rural categorization, mobility, physical objects, communication infrastructure, radio capable devices, interference, and so on. For instance, RIS can be used by the attackers to generate a fake multipath channel or absorb signals to misrepresent the coverage area [151]. While JSC has received significant attention from the design and optimization perspective, there is a glaring gap in the literature regarding its security provisioning. We believe that the PLS framework provided in Section III delivers the necessary structure which can be extended to cover the sensing aspect of wireless systems.

B. RIS-EMPOWERED SMART RADIO ENVIRONMENTS

As mentioned in Section III-B3, RIS has great potential for enhancing the security of wireless communications. However, despite its promise, there are significant challenges related to CSI acquisition, phase noise/errors, and channel correlation, that need to be addressed before its full potential can be realized. For instance, the joint active/passive beamforming at the transmitter and RIS, respectively, requires the CSI of the eavesdropper (w.r.t. transmitter and RIS) but given that eavesdroppers are often passive, this is not a reasonable assumption [158]. Related to this, there is the issue of outdated CSI and how it might impact the RIS's performance (in terms of capacity) which is tackled in [159], where the authors consider different (centralized and distributed) deployment scenarios. The obtained results show improved results for centralized architecture when RIS is closer to either communication node, while decentralized deployment leads to higher capacity when RISs are further away from these nodes. It should be kept in mind that the achievable capacity for any link is directly connected to PLS performance via its secrecy capacity. Another common assumption regarding RISs is the continuous nature of phase shifts that can be induced by its elements. However, as highlighted in [160], this is not the case. Rather, these phase shifts are intertwined with the amplitude response (or reflection coefficients) and, therefore, must be optimized jointly [161]. The results here also indicate that despite the imperfect assumption regarding phase shifts, the asymptotic results converge to the continuous phase shift capacity for a large number of reflecting elements suggesting that overall capacity or secrecy capacity gains in the case of PLS can still be achieved. The problem of phase errors from the perspective of diversity order is also investigated in [162], with the authors concluding that full diversity order can be achieved over independent fading channels with RIS as long as the absolute phase error is less than $\pi/2$. However, this raises the question regarding how valid the independent fading assumption itself is. Some recent works have attempted to tackle this issue, where [163] shows that the conventional independent and identically distributed (i.i.d.) Rayleigh fading model is not realistic for RIS and provides an alternate model for spatial correlation that can be used in future studies. This is then used as a baseline in [164] where temporal evolution of channel is also considered and degrees of freedom for finite spacing between the reflecting elements are analyzed. Their exact impact on the achievable capacity (or secrecy capacity), however, remains to be studied. An additional concern regarding RISs is their limited granularity in frequency domain due to lack of digital/RF chains. This can cause interference when users/networks use adjacent channels, leading to inadvertent disruption of communication and even limit the RIS's performance in terms of frequency-selective scheduling [165].

C. HIGHER FREQUENCY BANDS (MMWAVE AND SUB-THZ)

The rising popularity of augmented/virtual reality applications necessitates higher bandwidths to ensure a smooth quality of experience (QoE) for the users. However, the amount of spectrum in the conventional cellular bands (up to 6 GHz) is already crowded. Consequently, higher frequency bands including mmWave and THz have garnered increasingly more attention from both academia and industry. These frequency bands have significantly different propagation characteristics compared to sub-6 GHz frequencies, with severe propagation losses being observed [166]. Moreover, such systems will use extremely directional narrow beams. Apart from strengthening the communication, directional transmission has the inherent advantage of security from any attacker lying outside the beam [38], [167]. The security of such transmissions can be further strengthened by the use of multiple propagation paths [168] and spatio-temporal array architectures [169]. The narrow beams and directional transmission, however, render reliable connectivity very challenging due to their small coverage area. Given that applications such as virtual reality cannot afford a connection being dropped, it is understandable that the mmWave/THz systems will be complemented by sub-6 GHz bands rather than operating in a stand-alone manner.

As discussed in Section III-A1, various models including NWDP, FTR, and the different variants of κ-μ have been proposed to represent the fading in mmWave/THz frequency bands. While the studies in references [87]–[93] provide theoretical analyses of several PLS metrics under the aforementioned fading models, there is still a paucity of PLS techniques that leverage these generalized models to improve the security performance of wireless systems in the higher frequency bands. Moreover, PLS mechanisms are required which can support nodes operating at distinct frequency bands with significantly varying channel propagation characteristics.

D. VISIBLE LIGHT COMMUNICATION

With the revolution of the lighting industry and large unexploited visible light spectrum, visible light communication (VLC) has been proposed as an auspicious and disruptive technology for 5G and beyond based on low-cost light-emitting diodes (LEDs), where the light is used for both illumination and data communication purposes simultaneously. VLC systems are more immune against interference and less susceptible to security vulnerabilities which is inherited from the fact that light does not penetrate through any opaque objects such as walls [170]. Therefore, it is reasonable to consider the VLC channel perfectly secure, at the physical layer, in a single user and/or private room scenario. However, in public areas such as classrooms, libraries, hallways, or planes, securing VLC networks is required [171]. In these public areas, possible eavesdroppers may exist and try to attain confidential information [172]. As [170] points out, the fundamentals and techniques of PLS developed for conventional RF systems, discussed in Section III, cannot be directly applied to VLC systems. This is primarily due to: (1) the variability of the standard specifications in transmission protocols and modulation schemes, and (2) the more deterministic nature of VLC channels. As such, typical techniques such as coding, multi-antenna schemes, relays/cooperation, and authentication do not apply to VLC systems [173]. For a comprehensive study of literature on securing VLC systems, readers are referred to [170], where different types of VLC systems are studied considering different network parameters such as the characteristics of VLC channel, the availability of CSI, the geometry of the communication environment, and the type of signaling used.

E. NON-TERRESTRIAL NETWORKS

Academia, industry, and standardization bodies have increased their activities related to NTNs as a potential enabler for ubiquitous connectivity, with the users clamoring for reliable service and coverage irrespective of their location [174]. Empowered by various deployment options such as satellites, high altitude platform systems (HAPS), and unmanned aerial vehicles (UAVs), NTNs are primarily used to expand the coverage in order to deliver connectivity to regions that are unreachable by conventional networks (i.e., isolated areas, marine vessels, airplanes) [175]. As stated in [176], the unique characteristics of NTNs make the problem of ensuring secure communication different from that of purely terrestrial networks (TNs). NTNs (at least the satellites) are primarily deployed in LoS scenarios, where the reduced propagation losses lead to increased coverage footprint. However, the increased coverage footprint also results in greater vulnerability to eavesdropping attacks. In [177], the authors propose the use of polarization domain to effectively prevent the eavesdropper from detecting the communication signal. A dual-polarized antenna was designed in fixed downlink satellite communication that enabled legitimate receivers to obtain polarization information. A significant challenge in devising security mechanisms for NTN emerges in the case of hybrid networks, which comprise both terrestrial and non-terrestrial components [178]. This scenario is studied in [179], [180], where the former adapts relay selection and user scheduling to ensure confidentiality of the communication and the latter analyzes the secrecy performance of the link between a multi-antenna NTN and terrestrial recipients via multiple cooperative relays in the presence of several eavesdroppers.

F. ULTRA-RELIABLE LOW-LATENCY SECURE COMMUNICATIONS

5G introduced the mission-critical communication (MCC) paradigm under uRLLC services to facilitate applications such as industrial automation, smart grids, augmented/virtual reality and remote healthcare systems [181]. Apart from the obvious requirements related to reliability and latency, these applications also require high security owing to their critical nature. For instance, any manipulated/disrupted control message in applications such as remote surgery may lead to loss of life. Cryptography-based approaches may not be feasible since they violate the ultra-low latency requirement due to the high-complexity signal processing required by encryption/decryption and other key management and distribution tasks [23]. Meanwhile, the relatively short channel block-length also limits the usage of complicated encryption/decryption algorithms in MCC [19]. As a result, security at the PHY layer has garnered considerable attention as a tool to offer low-complexity security mechanisms and lightweight encryption schemes for MCC applications [182]. It should, however, be kept in mind that not all PLS methods are applicable to the MCC paradigm. For instance, multi-antenna-based beamforming techniques, discussed in Section III, require accurate CSI which is hard or infeasible to obtain in uRLLC due to the ultra-low latency requirement. In such cases, location-based beamforming provides a desirable alternative [23]. An interesting thing to note here is the inherent trade-off between reliability and latency, which renders optimizing both extremely difficult [183]. The work in [184] extends this optimization problem to also include security as an optimization parameter. Consequently, it is important to develop future PLS methods that take reliability and latency requirements as inherent constraints.

G. MASSIVE CONNECTIVITY AND IOT

IoT technology enables physical objects to sense, communicate, and perform certain actions on demand, which can facilitate a multitude of applications, such as smart home, smart city, and ITSs. Since IoT is becoming increasingly prevalent in our daily lives, the security of IoT network is indispensable. PLS techniques can improve the security of IoT networks from three main aspects: firstly, IoT devices may be fast-moving and continually switching between different APs/BSs. This will result in frequent authentication requests leading to a delay beyond the latency tolerance of next-generation scenarios/applications [22]. PLS simplifies the handshake process by using, for example, RF fingerprinting to provide a method of direct identification for the authentication process. Secondly, IoT is being deployed in all sectors at a massive scale which makes it difficult to efficiently distribute and manage the secret keys [185]. PLS offers an exciting alternative where all communicating nodes can directly extract the keys from their environment/channel, thus eliminating the need for key distribution and management. Lastly, IoT devices cannot afford complicated processing to maintain security [21]. While certain PLS methods such as beamforming [112], noise aggregation [186], cooperative jamming [187], and artificial noise injection [75] require additional hardware, processing, and energy resources, PLS also provides certain asymmetric PLS mechanisms where the load of designing a secure transmission is moved to BS/AP side and no additional processing is required at IoT node itself. That being said, most of the existing PLS mechanisms do not take into consideration the energy efficiency or try to jointly optimize it with security performance. The authors in [188], on the other hand, propose a user association approach that maximizes the secure throughput while minimizing energy consumption in an ultra-dense network. It is, therefore, likely that asymmetric, lightweight, and low-power PLS mechanisms will attain increasing popularity in next-generation networks provided their performance is validated in realistic settings.

H. PLS IN THE AGE OF EDGE COMPUTING

MEC is touted to be a potential enabler for both mMTC/IoT and uRLLC applications by reducing the need for backhaul bandwidth for the former and cutting down the latency for the latter. The transference of computing capabilities closer to the user means real-time applications such as extended reality (XR) can be realized without the signal having to traverse all the way to the center of the network. Similarly, the amount of data to be sent to the central network can be reduced by doing preliminary analysis/processing at the edge servers/devices. However, the presence of additional network nodes outside the physically secure information technology (IT) center of the network introduces vulnerabilities to the privacy of user data from potential eavesdroppers, necessitating PLS methods tailored to MEC scenarios. One such scheme involving transmission of jamming signals from MEC servers is given in [189], where full duplexing capability is used to mitigate self-interference. A deep learning (DL)-driven authentication mechanism using CSI fingerprint to counter any spoofing attacks is proposed in [190]. The impact of MEC on PLS, or how the former can enable and empower the latter, however, remains to be studied.

I. V2X COMMUNICATION

V2X communication encompasses different facets of vehicular communication depending on what the connected vehicle communicates with, including vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), vehicle-to-pedestrians (V2P) and vehicle-to-network (V2N). In general, vehicles and end devices interact and exchange data with each other in order to improve road safety. Therefore, they need to be connected in a reliable and timely manner, where the confidentiality and security of messages are vital [191]. V2X communication is particularly vulnerable to the data exchange being intercepted and private information about identity, position, and trajectory of the users being exposed [192]. PLS has been discussed as a potential solution to these problems [193]. However, one of the biggest challenges in this regard is to adapt to the varying security requirements as a function of the application, location, utility, environment, and other contextual information about the user. As [194] points out, it is not possible to provide appropriate security for different V2X applications and scenarios, suggesting applying different PLS techniques in a cooperative manner. An intelligent framework for this is provided in [18], however, any further studies or feasibility analysis of such an approach remains missing.

J. ADVERSARIAL ML AND EXPLAINABLE AI

The increasing complexity of wireless systems in terms of waveforms, propagation environments, and resource allocation has left the network operators and architects with no choice but to turn towards AI/ML to improve network performance. Some examples of this include the use of DL in Citizens Broadband Radio Service (CBRS) band to detect the presence of incumbent users, and the optimization of network slicing to improve network resource utilization. Both of these applications have shown to be vulnerable to adversarial ML, where the *black-box* nature of AI has been utilized to target the learning process and consequently render decisions adverse to the legitimate users/network [195]. Apart from approaches that involve pre-emptive training to mitigate possible adversarial attacks [196], [197], an alternative is to move towards explainable AI (XAI) to improve the level of users' trust towards such systems by providing interpretable explanations of the decisions taken by the machine. However, there remains a trade-off between explainability and performance for cases where mathematical models are absent [198]. Moreover, as [199] points out, unless the models are explicitly designed to be transparent, the explanation or interpretability remains a subjective function of the user's knowledge of the specific domain. Accordingly, it is important to design/tailor the AI/ML models with prior knowledge of the wireless communication domain.

K. CROSS-LAYER SECURITY

Typically, the network protocol stack layers are protected with a set of independent and uncoordinated security mechanisms ignoring their cross-layer interaction. However, independent security solutions at different layers might lead to conflicting actions and result in performance degradation. For instance, intricate attacks exploit multiple vulnerabilities of various layers leveraging isolation and lack of awareness and cooperation between them. Therefore, proper interaction and coordination among different protocol layers help in developing a robust detection system suitable for wireless networks. Such interactions are the key elements to building cross-layer architectures [200]. However, a limited number of works have been reported on this topic so far. For example, cross MAC/PHY layer security is proposed in [201]. Automatic repeat request (ARQ) (as MAC operation) and maximal-ratio combining (MRC) (as PHY operation) have been jointly exploited to enhance the confidentiality of wireless services requested by a legitimate user against eavesdropping attack. The potentials of application (APP) and PHY layers can also be explored to enhance security. Such as in [202] where employing authentication and watermarking strategies at the APP layer along with the coding and signal processing at the PHY layer can lead to considerable secrecy gains. Any further security interaction study between other layers and PHY layer remains missing.

V. CHALLENGES FOR PHYSICAL LAYER SECURITY

Despite the fruitful research in PLS era, there is a variety of challenges to be tackled in order to make PLS a reality. In this section, we provide and list several open issues and challenges for future works which are as follows:

- A major roadblock in the practical realization of PLS is the limiting assumptions often made regarding the attacking nodes. This may refer to the processing capabilities of the attacker, the number of antennas, active/passive, or individual/collaborative nature. This fact has slowed both the development of proof-of-concept prototypes and the acceptance of PLS approaches to security in reality [203]. Quite often, the attacker is assumed to be similar to a simple legitimate receiver in the network. While this assumption might be valid to ensure the privacy of wireless links from other users in the network, a malicious *attacker* should be considered to be suitably equipped and capable of smartly switching between different types of attacks based on link quality [204].
- For any observable parameter, reciprocity is imperative which has been assumed in this work. However, achieving this can be quite challenging in practical scenarios. For example, TDD system itself is reciprocal, but the channel estimation results at both ends of the link, which are affected by noise and interference may not be consistent [99]. Therefore, when the observable parameter is not the same at both ends, some information needs to be exchanged between the communicating entities for reciprocity compensation, resulting in the potential risk of observable parameter disclosure.
- 5G and beyond paradigms promise ubiquitous connectivity anytime, anywhere including high-speed scenarios. Mobility (particularly high-speed mobility) brings challenges such as Doppler spreading, selectivity of the channel, low coherence time, increased handovers and authentication overhead [205]. The channel selectivity and shorter coherence duration become a more pronounced problem from a PLS perspective. For instance, in PHY authentication if the legitimate transmitter and receiver lose their connection for more than coherence time, the channel no longer supports verification of the users [71]. In such cases, the authentication procedures need to be re-evaluated or even re-designed.
- With the increasing popularity of concepts such as cognitive/adaptive PLS and PLS for JSC, it is important

(and even imperative in some cases) to devise new metrics to quantify security for next-generation wireless networks. While link-level metrics for communication security have been extensively studied [206], there is limited work on quantifying the security of an environment. For instance, [207] proposes a "secrecy map" which provides average secrecy capacity over the whole space for given positions of legitimate nodes without putting any location constraints on the illegitimate node. Considering the importance being given to sensing in beyond 5G networks, it might be prudent to come up with security metrics that can be extended to cover the security of sensing and communication jointly for the whole environment instead of limiting it to specific scenarios in terms of attackers' and interferers' locations or orientations.

- So far, PLS approaches remain limited to the information theory domain, without practical implementations. A limited number of works have been triggering the practical validation of PLS approaches. For instance, the implementation of two PLS techniques is proposed in [208], namely phase enciphered Alamouti coding (PEAC) and artificial noise. The resulting testbed is very complex though, as well as difficult to replicate and validate. Besides, the implementation is only applicable to a situation where the Shannon capacity of the eavesdropper is exactly half the Shannon capacity of the legitimate receiver. However, a proof-of-concept using off-the-shelf hardware to protect the legitimate communication against mobile eavesdropping is proposed in [209]. This is achieved by leveraging the flexibility and control granularity offered by the relatively new concept of spectrum programming [210], by which it provides the ability to control and degrade the quality of the eavesdropper's channel by virtually manipulating the connectivity of the legitimate receiver.

VI. CONCLUSION

Wireless communication systems form a critical part of our lives, providing connectivity for various applications such as healthcare, education, trading, industrial automation, and transportation. The increased connectivity and coverage, though beneficial from a usefulness perspective, become a vulnerability in terms of user privacy and data confidentiality. Even though cryptographic methods are widely used for communication security, they are at risk with the advent of quantum computing. Moreover, the key management and distribution which is essential to cryptography cannot scale with the exploding heterogeneity of next-generation wireless devices. PLS offers a promising alternative, where properties of the wireless channel, RF front-end of the equipment, and physical parameters of the surrounding radio environment are exploited to ensure confidentiality, integrity, authenticity, and availability for the communication systems.

Despite PLS being a well-studied topic, a singular definition or unified framework describing the essential components (and their realizations) of PLS has been missing from the literature till now. In this work, we have described the general PLS framework comprising of observation and modification plane, where the former serves as the source of entropy while the latter illustrates how the transmissions can be modified to provide security. In addition to providing a clear distinction between cryptography and PLS, this framework not only allows the categorization of existing works but also makes room for the development of next-generation PLS methods. In line with this, the emerging technologies relevant to PLS have been highlighted along with potential challenges in realizing them.

REFERENCES

[1] Qualcomm Technologies Inc., "Making 5G NR a reality," White Paper, Dec. 2016.

[2] Intel Staff, "Top Use Cases for 5G Technology," Accessed Jan. 12, 2022. [Online]. Available: https://www.intel.com/content/www/us/en/wireless-network/5g-use-cases-applications.html

[3] M. Series, "IMT Vision-Framework and Overall Objectives of the Future Development of IMT for 2020 and Beyond," ITU Recommendation, 2015.

[4] 5G Infrastructure PPP Association, "5G Vision - The 5G Infrastructure Public Private Partnership: The Next Generation of Communication Networks and Services," White Paper, Feb. 2015.

[5] Amy Nordum, Kristen Clark and IEEE Spectrum Staff, Everything You Need to Know About 5G, Accessed: Aug. 3, 2020. [Online]. Available: https://spectrum.ieee.org/video/telecom/wireless/everything-you-need-to-know-about-5g

[6] A. A. Zaidi, R. Baldemair, H. Tullberg, H. Bjorkegren, L. Sundstrom, J. Medbo, C. Kilinc, and I. Da Silva, "Waveform and numerology to support 5G services and requirements," *IEEE Commun. Mag.*, vol. 54, no. 11, pp. 90–98, Nov. 2016.

[7] X. You, C. Zhang, X. Tan, S. Jin, and H. Wu, "AI for 5G: Research directions and paradigms," *Sci. China Inf. Sci.*, vol. 62, no. 2, pp. 1–13, 2019.

[8] Y. Sun, M. Peng, Y. Zhou, Y. Huang, and S. Mao, "Application of machine learning in wireless networks: Key techniques and open issues," *IEEE Commun. Surv. Tuts.*, vol. 21, no. 4, pp. 3072–3108, Oct.–Dec. 2019.

[9] Z. Zhang, Y. Xiao, Z. Ma, M. Xiao, Z. Ding, X. Lei, G. K. Karagiannidis, and P. Fan, "6G wireless networks: Vision, requirements, architecture, and key technologies," *IEEE Veh. Technol. Mag.*, vol. 14, no. 3, pp. 28–41, Sep. 2019.

[10] F. Tariq, M. R. Khandaker, K.-K. Wong, M. A. Imran, M. Bennis, and M. Debbah, "A speculative study on 6G," *IEEE Wireless Commun.*, vol. 27, no. 4, pp. 118–125, Aug. 2020.

[11] G. Gui, M. Liu, F. Tang, N. Kato, and F. Adachi, "6G: Opening new horizons for integration of comfort, security, and intelligence," *IEEE Wireless Commun.*, vol. 27, no. 5, pp. 126–132, Oct. 2020.

[12] F. Tang, Y. Kawamoto, N. Kato, and J. Liu, "Future intelligent and secure vehicular network toward 6G: Machine-learning approaches," *Proc. IEEE*, vol. 108, no. 2, pp. 292–307, Feb. 2020.

[13] A. Yazar, S. Dogan-Tusha, and H. Arslan, "6G vision: An ultra-flexible perspective," *ITU J. Future Evolving Technol.*, vol. 1, no. 1, pp. 121–140, 2020.

[14] A. Chorti *et al.*, "Context-aware security for 6G wireless the role of physical layer security," *IEEE Commun. Standards Mag.*, vol. 6, no. 1, pp. 102–108, 2022.

[15] M. Ylianttila *et al.*, "6G white paper: Research challenges for trust, security and privacy," 2020, *arXiv:2004.11665*.

[16] V. Mavroeidis, K. Vishi, M. D. Zych, and A. Jøsang, "The impact of quantum computing on present cryptography," 2018, *arXiv:1804.00200*.

[17] Q. Qi, X. Chen, C. Zhong, and Z. Zhang, "Physical layer security for massive access in cellular Internet of Things," *Sci. China Inf. Sci.*, vol. 63, no. 2, pp. 1–12, 2020.

[18] H. M. Furqan, M. S. J. Solaija, J. M. Hamamreh, and H. Arslan, "Intelligent physical layer security approach for V2X communication," 2019, *arXiv:1905.05075*.

[19] C. Li, C.-P. Li, K. Hosseini, S. B. Lee, J. Jiang, W. Chen, G. Horn, T. Ji, J. E. Smee, and J. Li, "5G-based systems design for tactile Internet," *Proc. IEEE*, vol. 107, no. 2, pp. 307–324, Feb. 2019.

[20] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey," *IEEE Commun. Surv. Tuts.*, vol. 21, no. 2, pp. 1773–1828, Apr.–Jun. 2018.

[21] N. Wang, P. Wang, A. Alipour-Fanid, L. Jiao, and K. Zeng, "Physical-layer security of 5G wireless networks for IoT: Challenges and opportunities," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8169–8181, Oct. 2019.

[22] K. Zeng, "Physical layer key generation in wireless networks: Challenges and opportunities," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 33–39, Jun. 2015.

[23] R. Chen, C. Li, S. Yan, R. Malaney, and J. Yuan, "Physical layer security for ultra-reliable and low-latency communications," *IEEE Wireless Commun.*, vol. 26, no. 5, pp. 6–11, Oct. 2019.

[24] M. Shakiba-Herfeh, A. Chorti, and H. V. Poor, "Physical layer security: Authentication, integrity, and confidentiality," in *Physical Layer Security*. Berlin, Germany: Springer, 2021, pp. 129–150.

[25] Y.-S. Shiu, S. Y. Chang, H.-C. Wu, S. C.-H. Huang, and H.-H. Chen, "Physical layer security in wireless networks: A tutorial," *IEEE Wireless Commun.*, vol. 18, no. 2, pp. 66–74, Apr. 2011.

[26] L. Wang and A. M. Wyglinski, "Detection of man-in-the-middle attacks using physical layer wireless security techniques," *Wireless Commun. Mobile Comput.*, vol. 16, no. 4, pp. 408–426, 2016.

[27] P. Hao, X. Wang, and A. Behnad, "Relay authentication by exploiting I/Q imbalance in amplify-and-forward system," in *Proc. IEEE Glob. Commun. Conf.*, 2014, pp. 613–618.

[28] Y. Chen, J. Yang, W. Trappe, and R. P. Martin, "Detecting and localizing identity-based attacks in wireless and sensor networks," *IEEE Trans. Veh. Technol.*, vol. 59, no. 5, pp. 2418–2434, Jun. 2010.

[29] N. Xie and S. Zhang, "Blind authentication at the physical layer under time-varying fading channels," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 7, pp. 1465–1479, Jul. 2018.

[30] G. Chen and W. Dong, "Jamcloak: Reactive jamming attack over cross-technology communication links," in *Proc. IEEE 26th Int. Conf. Netw. Protoc.*, 2018, pp. 34–43.

[31] L. Hao, T. Li, and Q. Ling, "A highly efficient secure communication interface: Collision-free frequency hopping (CFFH)," in *Proc. Workshop Signal Process. Appl. Public Secur. Forensics*, 2007, pp. 1–4.

[32] X. Cheng and B. Huang, "A center-based secure and stable clustering algorithm for VANETs on highways," *Wireless Commun. Mobile Comput.*, vol. 2019, pp. 1–10, 2019.

[33] N. Komninos, E. Philippou, and A. Pitsillides, "Survey in smart grid and smart home security: Issues, challenges and countermeasures," *IEEE Commun. Surv. Tut.*, vol. 16, no. 4, pp. 1933–1954, Oct./Dec. 2014.

[34] S. Soltan, P. Mittal, and H. V. Poor, "BlackIoT: IoT botnet of high wattage devices can disrupt the power grid," in *Proc. 27th USENIX Secur. Symp.*, 2018, pp. 15–32.

[35] M. Stanislav and T. Beardsley, "Hacking IoT: A. case study on baby monitor exposures and vulnerabilities," 2015. [Online]. Available: https://www.rapid7.com/globalassets/external/docs/Hacking-Iot-A-Case-Study-on-Baby-Monitor-Exposures-and-Vulnerabilities.pdf

[36] R. F. Schaefer, H. Boche, and H. V. Poor, "Secure communication under channel uncertainty and adversarial attacks," *Proc. IEEE*, vol. 103, no. 10, pp. 1796–1813, Oct. 2015.

[37] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proc. IEEE*, vol. 104, no. 9, pp. 1727–1765, Sep. 2016.

[38] 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. 36, no. 4, pp. 679–695, Apr. 2018.

[39] Y. Liu, H.-H. Chen, and L. Wang, "Physical layer security for next generation wireless networks: Theories, technologies, and challenges," *IEEE Commun. Surv. Tut.*, vol. 19, no. 1, pp. 347–376, Jan.–Mar. 2017.

[40] L. Sun and Q. Du, "Physical layer security with its applications in 5G networks: A review," *China Commun.*, vol. 14, no. 12, pp. 1–14, Dec. 2017.

[41] W. Wang, Z. Sun, S. Piao, B. Zhu, and K. Ren, "Wireless physical-layer identification: Modeling and validation," *IEEE Trans. Inf. Forensics Secur.*, vol. 11, no. 9, pp. 2091–2106, Sep. 2016.

[42] O. Gungor, F. Chen, and C. E. Koksal, "Secret key generation via localization and mobility," *IEEE Trans. Veh. Technol.*, vol. 64, no. 6, pp. 2214–2230, Jun. 2015.

[43] L. Mucchi, S. Caputo, P. Marcocci, G. Chisci, L. Ronga, and E. Panayirci, "Security and reliability performance of noise-loop modulation: Theoretical analysis and experimentation," *IEEE Trans. Veh. Technol.*, to be published, doi: 10.1109/TVT.2022.3160094.

[44] K. Grover, A. Lim, and Q. Yang, "Jamming and anti-jamming techniques in wireless networks: A survey," *Int. J. Ad Hoc Ubiquitous Comput.*, vol. 17, no. 4, pp. 197–215, 2014.

[45] H. Pirayesh and H. Zeng, "Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey," *IEEE Commun. Surv. Tut.*, vol. 24, no. 2, pp. 767–809, Apr.–Jun. 2022.

[46] W. Li, D. Mclernon, J. Lei, M. Ghogho, S. A. R. Zaidi, and H. Hui, "Cryptographic primitives and design frameworks of physical layer encryption for wireless communications," *IEEE Access*, vol. 7, pp. 63660–63673, 2019.

[47] R. Ma, L. Dai, Z. Wang, and J. Wang, "Secure communication in TDS-OFDM system using constellation rotation and noise insertion," *IEEE Trans. Consum. Electron.*, vol. 56, no. 3, pp. 1328–1332, Aug. 2010.

[48] D. Park, J. Ahn, C. Choe, S. Woo, S. Ahn, and J. Choi, "A noise-shaped signaling method for vehicle-to-everything security," *IEEE Access*, vol. 9, pp. 75385–75397, 2021.

[49] B. Chen, C. Zhu, W. Li, J. Wei, V. C. Leung, and L. T. Yang, "Original symbol phase rotated secure transmission against powerful massive MIMO eavesdropper," *IEEE Access*, vol. 4, pp. 3016–3025, 2016.

[50] D. Xu, P. Ren, Q. Du, L. Sun, and Y. Wang, "Physical layer security improvement by constellation selection and artificial interference," in *Wireless Commun. Netw. Conf.*, 2017, pp. 1–6.

[51] J. M. Hamamreh, E. Basar, and H. Arslan, "OFDM-subcarrier index selection for enhancing security and reliability of 5G URLLC services," *IEEE Access*, vol. 5, pp. 25863–25875, 2017.

[52] H. M. Furqan, J. M. Hamamreh, and H. Arslan, "Enhancing physical layer security of OFDM systems using channel shortening," in *28th Annu. Int. Symp. Personal, Indoor, Mobile Radio Commun. (PIMRC)*. IEEE, 2017, pp. 1–5.

[53] H. M. Furqan, J. M. Hamamreh, and H. Arslan, "New physical layer key generation dimensions: Subcarrier indices/positions-based key generation," *IEEE Commun. Lett.*, vol. 25, no. 1, pp. 59–63, Jan. 2021.

[54] J. M. Hamamreh, Z. E. Ankarali, and H. Arslan, "CP-less OFDM with alignment signals for enhancing spectral efficiency, reducing latency, and improving PHY security of 5G services," *IEEE Access*, vol. 6, pp. 63649–63663, 2018.

[55] B. He, Y. She, and V. K. Lau, "Artificial noise injection for securing single-antenna systems," *IEEE Trans. Veh. Technol.*, vol. 66, no. 10, pp. 9577–9581, Oct. 2017.

[56] Y. Wu, C. Xiao, Z. Ding, X. Gao, and S. Jin, "Linear precoding for finite-alphabet signaling over MIMOME wiretap channels," *IEEE Trans. Veh. Technol.*, vol. 61, no. 6, pp. 2599–2612, Jul. 2012.

[57] X. Li, H.-N. Dai, M. K. Shukla, D. Li, H. Xu, and M. Imran, "Friendly-jamming schemes to secure ultra-reliable and low-latency communications in 5G and beyond communications," *Comput. Standards Interfaces*, vol. 78, 2021, Art. no. 103540.

[58] M. Yang, B. Zhang, Y. Huang, N. Yang, D. Guo, and B. Gao, "Secure multiuser communications in wireless sensor networks with TAS and cooperative jamming," *Sensors*, vol. 16, no. 11, 2016, Art. no. 1908.

[59] C. Wang and Z. Wang, "Signal alignment for secure underwater coordinated multipoint transmissions," *IEEE Trans. Signal Process.*, vol. 64, no. 23, pp. 6360–6374, Dec. 2016.

[60] L. Peng, A. Hu, J. Zhang, Y. Jiang, J. Yu, and Y. Yan, "Design of a hybrid RF fingerprint extraction and device classification scheme," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 349–360, Feb. 2019.

[61] W. Li, N. Wang, L. Jiao, and K. Zeng, "Physical layer spoofing attack detection in MmWave massive MIMO 5G networks," *IEEE Access*, vol. 9, pp. 60419–60432, 2021.

[62] X. Li, K. Huang, S. Wang, and X. Xu, "A physical layer authentication mechanism for IoT devices," *China Commun.*, vol. 19, no. 5, pp. 129–140, May 2022.

[63] Y. An, S. Zhang, and Z. Ji, "A tag-based PHY-layer authentication scheme without key distribution," *IEEE Access*, vol. 9, pp. 85947–85955, 2021.

[64] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

[65] Q. Wang, H. Zhang, Q. Lyu, X. Wang, and J. Bao, "A novel physical channel characteristics-based channel hopping scheme for jamming-resistant in wireless communication," *Int. J. Netw. Secur.*, vol. 20, no. 3, pp. 439–446, 2018.

[66] G. Noubir, "On connectivity in ad hoc networks under jamming using directional antennas and mobility," in *Proc. Int. Conf. Wired/Wireless Internet Commun.*, 2004, pp. 186–200.

[67] H. Yang *et al.*, "Intelligent reflecting surface assisted anti-jamming communications: A fast reinforcement learning approach," *IEEE Trans. Wireless Commun.*, vol. 20, no. 3, pp. 1963–1974, Mar. 2021.

[68] M. K. Ozdemir and H. Arslan, "Channel estimation for wireless OFDM systems," *IEEE Commun. Surv. Tut.*, vol. 9, no. 2, pp. 18–48, Apr.–Jun. 2007.

[69] A. B. Kihero, A. Tusha, and H. Arslan, "Wireless channel and interference," in *Wireless Communication Signals: A Laboratory-Based Approach*. Hoboken, NJ, USA: Wiley, 2021, pp. 267–323.

[70] D. Marabissi, L. Mucchi, and A. Stomaci, "IoT nodes authentication and ID spoofing detection based on joint use of physical layer security and machine learning," *Future Internet*, vol. 14, no. 2, 2022, Art. no. 61.

[71] W. Trappe, "The challenges facing physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 16–20, Jun. 2015.

[72] H. Khodakarami and F. Lahouti, "Link adaptation for physical layer security over wireless fading channels," *IET Commun.*, vol. 6, no. 3, pp. 353–362, 2012.

[73] Y. E. H. Shehadeh and D. Hogrefe, "A survey on secret key generation mechanisms on the physical layer in wireless networks," *Secur. Commun. Netw.*, vol. 8, no. 2, pp. 332–341, 2015.

[74] L. Y. Paul, J. S. Baras, and B. M. Sadler, "Physical-layer authentication," *IEEE Trans. Inf. Forensics Secur.*, vol. 3, no. 1, pp. 38–51, Mar. 2008.

[75] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.

[76] S. Kundu, D. A. Pados, and S. N. Batalama, "Hybrid-ARQ as a communications security measure," in *Proc. Int. Conf. Acoust., Speech Signal Process.*, 2014, pp. 5681–5685.

[77] J. M. Hamamreh and H. Arslan, "Secure orthogonal transform division multiplexing (OTDM) waveform for 5G and beyond," *IEEE Commun. Lett.*, vol. 21, no. 5, pp. 1191–1194, May 2017.

[78] J. Zhang, T. Q. Duong, A. Marshall, and R. Woods, "Key generation from wireless channels: A review," *IEEE Access*, vol. 4, pp. 614–626, 2016.

[79] L. Xiao, L. J. Greenstein, N. B. Mandayam, and W. Trappe, "Using the physical layer for wireless authentication in time-variant channels," *IEEE Trans. Wireless Commun.*, vol. 7, no. 7, pp. 2571–2579, Jul. 2008.

[80] M. K. Samimi, G. R. MacCartney, S. Sun, and T. S. Rappaport, "28 GHz millimeter-wave ultrawideband small-scale fading models in wireless channels," in *Proc. 83rd Veh. Technol. Conf.*, 2016, pp. 1–6.

[81] E. N. Papasotiriou, A.-A. A. Boulogeorgos, K. Haneda, M. F. de Guzman, and A. Alexiou, "An experimentally validated fading model for THz wireless systems," *Sci. Rep.*, vol. 11, no. 1, pp. 1–14, 2021.

[82] Y. Xing, T. S. Rappaport, and A. Ghosh, "Millimeter wave and sub-THz indoor radio propagation channel measurements, models, and comparisons in an office environment," *IEEE Commun. Lett.*, vol. 25, no. 10, pp. 3151–3155, Oct. 2021.

[83] G. D. Durgin, T. S. Rappaport, and D. A. De Wolf, "New analytical models and probability density functions for fading in wireless communications," *IEEE Trans. Commun.*, vol. 50, no. 6, pp. 1005–1015, Jun. 2002.

[84] J. D. V. Sánchez, D. P. M. Osorio, F. J. Löpez-Martınez, M. C. P. Paredes, and L. F. Urquiza-Aguiar, "On the secrecy performance over N-wave with diffuse power fading channel," *IEEE Trans. Veh. Technol.*, vol. 69, no. 12, pp. 15137–15148, Dec. 2020.

[85] J. M. Romero-Jerez, F. J. Lopez-Martinez, J. F. Paris, and A. J. Goldsmith, "The fluctuating two-ray fading model: Statistical characterization and performance analysis," *IEEE Trans. Wireless Commun.*, vol. 16, no. 7, pp. 4420–4432, Jul. 2017.

[86] W. Zeng, J. Zhang, S. Chen, K. P. Peppas, and B. Ai, "Physical layer security over fluctuating two-ray fading channels," *IEEE Trans. Veh. Technol.*, vol. 67, no. 9, pp. 8949–8953, Sep. 2018.

[87] N. Bhargav, S. L. Cotton, and D. E. Simmons, "Secrecy capacity analysis over $\kappa - \mu$ fading channels: Theory and applications," *IEEE Trans. Commun.*, vol. 64, no. 7, pp. 3011–3024, Jul. 2016.

[88] S. Iwata, T. Ohtsuki, and P.-Y. Kam, "Secure outage probability over $\kappa - \mu$ fading channels," in *Int. Conf. Commun.*, 2017, pp. 1–6.

[89] J. M. Moualeu and W. Hamouda, "On the secrecy performance analysis of SIMO systems over $\kappa - \mu$ fading channels," *IEEE Commun. Lett.*, vol. 21, no. 11, pp. 2544–2547, Nov. 2017.

[90] J. D. V. Sánchez, D. P. M. Osorio, F. J. López-Martınez, M. C. P. Paredes, and L. F. Urquiza-Aguiar, "Information-theoretic security of MIMO networks under $\kappa - \mu$ shadowed fading channels," *IEEE Trans. Veh. Technol.*, vol. 70, no. 7, pp. 6302–6318, Jul. 2021.

[91] J. M. Moualeu, D. B. da Costa, W. Hamouda, U. S. Dias, and R. A. de Souza, "Physical layer security over $\alpha - \kappa - \mu$ and $\alpha - \eta - \mu$ fading channels," *IEEE Trans. Veh. Technol.*, vol. 68, no. 1, pp. 1025–1029, Jan. 2019.

[92] T. R. R. Marins *et al.*, "Fading evaluation in the mm-Wave band," *IEEE Trans. Commun.*, vol. 67, no. 12, pp. 8725–8738, Dec. 2019.

[93] A. Mathur, Y. Ai, M. R. Bhatnagar, M. Cheffena, and T. Ohtsuki, "On physical layer security of $\alpha - \eta - \kappa - \mu$ fading channels," *IEEE Commun. Lett.*, vol. 22, no. 10, pp. 2168–2171, Oct. 2018.

[94] P. Yadav, S. Kumar, and R. Kumar, "A comprehensive survey of physical layer security over fading channels: Classifications, applications, and challenges," *Trans. Emerg. Telecommun. Technol.*, vol. 32, no. 9, 2021, Art. no. e4270.

[95] H. Arslan, "RF Impairments," in *Wireless Communication Signals: A Laboratory-Based Approach*. Newark, NJ, USA: Wiley, 2021, pp. 99–120.

[96] J. Zhang, S. Rajendran, Z. Sun, R. Woods, and L. Hanzo, "Physical layer security for the Internet of Things: Authentication and key generation," *IEEE Wireless Commun.*, vol. 26, no. 5, pp. 92–98, Oct. 2019.

[97] P. Hao and X. Wang, "Performance enhanced wireless device authentication using multiple weighted device-specific characteristics," in *China Summit Int. Conf. Signal Inf. Process.*, 2015, pp. 438–442.

[98] X. Wang, P. Hao, and L. Hanzo, "Physical-layer authentication for wireless security enhancement: Current challenges and future developments," *IEEE Commun. Mag.*, vol. 54, no. 6, pp. 152–158, Jun. 2016.

[99] L. Zhao, X. Zhang, J. Chen, and L. Zhou, "Physical layer security in the age of artificial intelligence and edge computing," *IEEE Wireless Commun.*, vol. 27, no. 5, pp. 174–180, Oct. 2020.

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

[101] M. Karabacak, B. PekÖz, G. Mumcu, and H. Arslan, "Arraymetrics: Authentication through chaotic antenna array geometries," *IEEE Commun. Lett.*, vol. 25, no. 6, pp. 1801–1804, Jun. 2021.

[102] L. Afeef, H. M. Furqan, and H. Arslan, "Physical layer authentication scheme in beamspace MIMO systems," *IEEE Commun. Lett.*, to be published, doi: 10.1109/LCOMM.2022.3170509.

[103] A. Badawy, T. Elfouly, T. Khattab, A. Mohamed, and M. Guizani, "Unleashing the secure potential of the wireless physical layer: Secret key generation methods," *Phys. Commun.*, vol.19, pp. 1–10, 2016.

[104] A. Badawy, T. Khattab, T. El-Fouly, A. Mohamed, D. Trinchero, and C.-F. Chiasserini, "Secret key generation based on AoA estimation for low SNR conditions," in *Proc. 81st Veh. Technol. Conf.*, 2015, pp. 1–7.

[105] C. Perkins *et al.*, "Distance sensing for mini-robots: RSSI vs. TDOA," in *Proc. Int. Symp. Circuits Syst.*, 2011, pp. 1984–1987.

[106] A. Badawy, T. Khattab, T. ElFouly, A. Mohamed, and D. Trinchero, "Secret key generation based on channel and distance measurements," in *Proc. 6th Int. Congr. Ultra Modern Telecommun. Control Syst. Workshops*, 2014, pp. 136–142.

[107] R. L. Rivest, "Cryptography," in *Handbook of Theoretical Computer Science*, Volume A, J. Van Leeuwen and J. Leeuwen, Eds., Elsevier, 1990, ch. 13, pp. 718–755.

[108] L. Jiao, N. Wang, P. Wang, A. Alipour-Fanid, J. Tang, and K. Zeng, "Physical layer key generation in 5G wireless networks," *IEEE Wireless Commun.*, vol. 26, no. 5, pp. 48–54, Oct. 2019.

[109] H. Mahdavifar and A. Vardy, "Achieving the secrecy capacity of wiretap channels using polar codes," *IEEE Trans. Inf. Theory*, vol. 57, no. 10, pp. 6428–6443, Oct. 2011.

[110] A. Thangaraj, S. Dihidar, A. R. Calderbank, S. W. McLaughlin, and J.-M. Merolla, "Applications of LDPC codes to the wiretap channel," *IEEE Trans. Inf. Theory*, vol. 53, no. 8, pp. 2933–2945, Aug. 2007.

[111] H. M. Furqan, J. M. Hamamreh, and H. Arslan, "Physical layer security designs for 5G and beyond," in *Flexible and Cognitive Radio Access Technologies for 5G and Beyond*, H. Arslan and E. Basar, Eds., London, U.K.: IET, 2020, ch. 18, pp. 545–587.

[112] X. Chen, D. W. K. Ng, W. H. Gerstacker, and H.-H. Chen, "A survey on multiple-antenna techniques for physical layer security," *IEEE Commun. Surv. Tut.*, vol. 19, no. 2, pp. 1027–1053, Apr.–Jun. 2016.

[113] Z. Rezki and M.-S. Alouini, "On the finite-SNR diversity-multiplexing tradeoff of zero-forcing transmit scheme under secrecy constraint," in *Int. Conf. Commun. Workshops*, 2011, pp. 1–5.

[114] M. Pei, L. Wang, and D. Ma, "Linear MMSE transceiver optimization for general MIMO wiretap channels with QoS constraints," in *Int. Conf. Commun. China*, 2013, pp. 259–263.

[115] L. Zhang, Y. Cai, B. Champagne, and M. Zhao, "Tomlinson-Harashima precoding design in MIMO wiretap channels based on the MMSE criterion," in *Int. Conf. Commun. Workshop*, 2015, pp. 470–474.

[116] R. Liu, T. Liu, H. V. Poor, and S. Shamai, "MIMO Gaussian broadcast channels with confidential and common messages," in *Int. Symp. Inf. Theory*, 2010, pp. 2578–2582.

[117] Z. Li, W. Trappe, and R. Yates, "Secret communication via multi-antenna transmission," in *Proc. 41st Annu. Conf. Inf. Sci. Syst.*, 2007, pp. 905–910.

[118] A. Khisti, G. Wornell, A. Wiesel, and Y. Eldar, "On the Gaussian MIMO wiretap channel," in *Int. Symp. Inf. Theory*, 2007, pp. 2471–2475.

[119] S. Liu, Y. Hong, and E. Viterbo, "Practical secrecy using artificial noise," *IEEE Commun. Lett.*, vol. 17, no. 7, pp. 1483–1486, Jul. 2013.

[120] T. Xiong, W. Lou, J. Zhang, and H. Tan, "MIO: Enhancing wireless communications security through physical layer multiple inter-symbol obfuscation," *IEEE Trans. Inf. Forensics Secur.*, vol. 10, no. 8, pp. 1678–1691, Aug. 2015.

[121] S. Althunibat, V. Sucasas, and J. Rodriguez, "A physical-layer security scheme by phase-based adaptive modulation," *IEEE Trans. Veh. Technol.*, vol. 66, no. 11, pp. 9931–9942, Nov. 2017.

[122] S. E. Zegrar, H. M. Furqan, and H. Arslan, "Flexible physical layer security for joint data and pilots in future wireless networks," *IEEE Trans. Commun.*, vol. 70, no. 4, pp. 2635–2647, Apr. 2022.

[123] M. Yusuf and H. Arslan, "Controlled inter-carrier interference for physical layer security in OFDM systems," in *84th Veh. Technol. Conf.*, 2016, pp. 1–5.

[124] N. Van Huynh, D. N. Nguyen, D. T. Hoang, and E. Dutkiewicz, "Jam me if you can: Defeating jammer with deep dueling neural network architecture and ambient backscattering augmented communication," *IEEE J. Sel. Areas Commun.*, vol. 37, no. 11, pp. 2603–2620, Nov. 2019.

[125] P. Zhang, J. Liu, Y. Shen, H. Li, and X. Jiang, "Lightweight tag-based PHY-layer authentication for IoT devices in smart cities," *IEEE Internet Things J.*, vol. 7, no. 5, pp. 3977–3990, May 2020.

[126] A. Nosratinia, T. E. Hunter, and A. Hedayat, "Cooperative communication in wireless networks," *IEEE Commun. Mag.*, vol. 42, no. 10, pp. 74–80, Oct. 2004.

[127] K. R. Liu, A. K. Sadek, W. Su, and A. Kwasinski, *Cooperative Communications and Networking*. Cambridge, U.K.: Cambridge Univ. Press, 2009.

[128] F. Jameel, S. Wyne, G. Kaddoum, and T. Q. Duong, "A comprehensive survey on cooperative relaying and jamming strategies for physical layer security," *IEEE Commun. Surv. Tut.*, vol. 21, no. 3, pp. 2734–2771, Jul.–Sep. 2018.

[129] R. Zhao, X. Tan, D.-H. Chen, Y.-C. He, and Z. Ding, "Secrecy performance of untrusted relay systems with a full-duplex jamming destination," *IEEE Trans. Veh. Technol.*, vol. 67, no. 12, pp. 11511–11524, Dec. 2018.

[130] M. S. J. Solaija, H. M. Furqan, Z. E. Ankarali, and H. Arslan, "Cyclic prefix (CP) jamming against eavesdropping relays in OFDM systems," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, 2022, pp. 1976–1980, doi: 10.1109/WCNC51071.2022.9771587.

[131] *3rd Generation Partnership Project (3GPP)*, "Coordinated Multipoint Operation for LTE Physical Layer Aspects (Rel-11)," Technical Rep. 36.819, *ver 11.2.0*, Sep. 2013.

[132] M. S. J. Solaija, H. Salman, A. B. Kihero, M. İ. Sağlam, and H. Arslan, "Generalized coordinated multipoint framework for 5G and beyond," *IEEE Access*, vol. 9, pp. 72499–72515, 2021.

[133] M. Yusuf and H. Arslan, "Secure multi-user transmission using CoMP directional modulation," in *Proc. 82nd Veh. Technol. Conf.*, 2015, pp. 1–2.

[134] M. Hafez, M. Yusuf, T. Khattab, T. Elfouly, and H. Arslan, "Secure spatial multiple access using directional modulation," *IEEE Trans. Wireless Commun.*, vol. 17, no. 1, pp. 563–573, Jun. 2018.

[135] L. Xiao, X. Wan, and Z. Han, "PHY-layer authentication with multiple landmarks with reduced overhead," *IEEE Trans. Wireless Commun.*, vol. 17, no. 3, pp. 1676–1687, Mar. 2018.

[136] A. D. Wyner, "The wire-tap channel," *Bell System Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.

[137] M. Di Renzo *et al.*, "Smart radio environments empowered by reconfigurable intelligent surfaces: How it works, state of research, and the road ahead," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 11, pp. 2450–2525, Nov. 2020.

[138] M. Alayasra and H. Arslan, "IRS-enabled beam-space channel," *IEEE Trans. Wireless Commun.*, vol. 21, no. 6, pp. 3822–3835, Jun. 2021.

[139] A. Almohamad *et al.*, "Smart and secure wireless communications via reflecting intelligent surfaces: A short survey," *IEEE Open J. Commun. Soc.*, vol. 1, pp. 1442–1456, 2020.

[140] M. Cui, G. Zhang, and R. Zhang, "Secure wireless communication via intelligent reflecting surface," *IEEE Wireless Commun. Lett.*, vol. 8, no. 5, pp. 1410–1414, Oct. 2019.

[141] J. Qiao and M.-S. Alouini, "Secure transmission for intelligent reflecting surface-assisted mmWave and terahertz systems," *IEEE Wireless Commun. Lett.*, vol. 9, no. 10, pp. 1743–1747, Oct. 2020.

[142] X. Guan, Q. Wu, and R. Zhang, "Intelligent reflecting surface assisted secrecy communication: Is artificial noise helpful or not?," *IEEE Wireless Commun. Lett.*, vol. 9, no. 6, pp. 778–782, Jun. 2020.

[143] A. U. Makarfi *et al.*, "Reconfigurable intelligent surfaces-enabled vehicular networks: A physical layer security perspective," 2020, *arXiv:2004.11288*.

[144] M. H. Khoshafa, T. M. Ngatched, and M. H. Ahmed, "Reconfigurable intelligent surfaces-aided physical layer security enhancement in D2D underlay communications," *IEEE Commun. Lett.*, vol. 25, no. 5, pp. 1443–1447, May 2021.

[145] U. Altun and E. Basar, "Ris enabled secure communication with covert constraint," in *Proc. 55th Asilomar Conf. Signals, Systems, Comput.*, 2021, pp. 685–689.

[146] B. Kim, T. Erpek, Y. E. Sagduyu, and S. Ulukus, "Covert communications via adversarial machine learning and reconfigurable intelligent surfaces," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, 2022, pp. 411–416, doi: 10.1109/WCNC51071.2022.9771899.

[147] H. Du *et al.*, "Reconfigurable intelligent surface-aided joint radar and covert communications: Fundamentals, optimization, and challenges," 2022, *arXiv:2203.02704*.

[148] J. Hu, X. Shi, S. Yan, Y. Chen, T. Zhao, and F. Shu, "Hybrid relay-reflecting intelligent surface-aided covert communications," 2022, *arXiv:2203.12223*.

[149] G. Li *et al.*, "Reconfigurable intelligent surface for physical layer key generation: Constructive or destructive?" *IEEE Wireless Commun.*, to be published, doi: 10.1109/MWC.007.2100545.

[150] M. H. Yilmaz, E. Güvenkaya, H. M. Furqan, S. KÖse, and H. Arslan, "Cognitive security of wireless communication systems in the physical layer," *Wireless Commun. Mobile Comput.*, vol. 2017, pp. 1–9, 2017.

[151] H. M. Furqan, M. S. J. Solaija, H. Türkmen, and H. Arslan, "Wireless communication, sensing, and REM: A security perspective," *IEEE Open J. Commun. Soc.*, vol. 2, pp. 287–321, 2021.

[152] B. Wang and N. Z. Gong, "Stealing hyperparameters in machine learning," in *Proc. Symp. Secur. Privacy*, 2018, pp. 36–52.

[153] F. Liu, C. Masouros, A. P. Petropulu, H. Griffiths, and L. Hanzo, “Joint radar and communication design: Applications, state-of-the-art, and the road ahead,” *IEEE Trans. Commun.*, vol. 68, no. 6, pp. 3834–3862, Jun. 2020.

[154] H. Türkmen, M. S. J. Solaija, A. Tusha, and H. Arslan, “Wireless sensing — enabler of future wireless technologies,” *Turkish J. Elect. Eng. Comput. Sci.*, vol. 29, no. 1, pp. 1–17, 2021.

[155] D. E. Lawrence, “Low probability of intercept antenna array beamforming,” *IEEE Trans. Antennas Propag.*, vol. 58, no. 9, pp. 2858–2865, Sep. 2010.

[156] Y. Shoukry, P. Martin, Y. Yona, S. Diggavi, and M Srivastava, “Py-CRA: Physical challenge-response authentication for active sensors under spoofing attacks,” in *Proc. 22nd ACM SIGSAC Conf. Comput. Commun. Secur.*, 2015, pp. 1004–1015.

[157] A. G. Fragkiadakis, E. Z. Tragos, and I. G. Askoxylakis, “A survey on security threats and detection techniques in cognitive radio networks,” *IEEE Commun. Surv. Tut.*, vol. 15, no. 1, pp. 428–445, Jan.–Mar. 2013.

[158] Y. Liu *et al.*, “Reconfigurable intelligent surfaces: Principles and opportunities,” *IEEE Commun. Surv. Tut.*, vol. 23, no. 3, pp. 1546–1577, Jul.–Sep. 2021.

[159] Y. Zhang, J. Zhang, M. Di Renzo, H. Xiao, and B. Ai, “Reconfigurable intelligent surfaces with outdated channel state information: Centralized vs. distributed deployments,” *IEEE Trans. Commun.*, vol. 70, no. 4, pp. 2742–2756, Apr. 2022.

[160] S. Abeywickrama, R. Zhang, Q. Wu, and C. Yuen, “Intelligent reflecting surface: Practical phase shift model and beamforming optimization,” *IEEE Trans. Commun.*, vol. 68, no. 9, pp. 5849–5863, Sep. 2020.

[161] Y. Zhang, J. Zhang, M. Di Renzo, H. Xiao, and B. Ai, “Performance analysis of RIS-aided systems with practical phase shift and amplitude response,” *IEEE Trans. Veh. Technol.*, vol. 70, no. 5, pp. 4501–4511, May 2021.

[162] I. Trigui, W. Ajib, W.-P. Zhu, and M. Di Renzo, “Performance evaluation and diversity analysis of RIS-assisted communications over generalized fading channels in the presence of phase noise,” *IEEE Open J. Commun. Soc.*, vol. 3, pp. 593–607, 2022.

[163] E. BjÖrnson and L. Sanguinetti, “Rayleigh fading modeling and channel hardening for reconfigurable intelligent surfaces,” *IEEE Wireless Commun. Lett.*, vol. 10, no. 4, pp. 830–834, Apr. 2021.

[164] S. Sun and H. Yan, “Small-scale spatial-temporal correlation and degrees of freedom for reconfigurable intelligent surfaces,” *IEEE Wireless Commun. Lett.*, vol. 10, no. 12, pp. 2698–2702, Dec. 2021.

[165] R. Liu, Q. Wu, M. Di Renzo, and Y. Yuan, “A path to smart radio environments: An industrial viewpoint on reconfigurable intelligent surfaces,” *IEEE Wireless Commun.*, vol. 29, no. 1, pp. 202–208, Feb. 2022.

[166] S. Rangan, T. S. Rappaport, and E. Erkip, “Millimeter-wave cellular wireless networks: Potentials and challenges,” *Proc. IEEE*, vol. 102, no. 3, pp. 366–385, Mar. 2014.

[167] Y. Zhu, L. Wang, K.-K. Wong, and R. W. Heath, “Physical layer security in large-scale millimeter wave ad hoc networks,” in *Proc. Glob. Commun. Conf.*, 2016, pp. 1–6.

[168] V. Petrov, D. Moltchanov, J. M. Jornet, and Y. Koucheryavy, “Exploiting multipath terahertz communications for physical layer security in beyond 5G networks,” in *Proc. Conf. Comput. Commun. Workshops*, 2019, pp. 865–872.

[169] K. Sengupta, X. Lu, S. Venkatesh, and B. Tang, “Physically secure sub-THz wireless links,” in *Int. Conf. Commun. Workshops*, 2020, pp. 1–7.

[170] M. A. Arfaoui *et al.*, “Physical layer security for visible light communication systems: A survey,” *IEEE Commun. Surv. Tut.*, vol. 22, no. 3, pp. 1887–1908, Jul.–Sep. 2020.

[171] Y. Liang, H. V. Poor, and S. Shamai, “Physical layer security in broadcast networks,” *Secur. Commun. Netw.*, vol. 2, no. 3, pp. 227–238, 2009.

[172] A. Mostafa and L. Lampe, “Enhancing the security of VLC links: Physical-layer approaches,” in *Proc. Summer Topicals Meeting Ser.*, 2015, pp. 39–40.

[173] L. Mucchi *et al.*, “Physical-layer security in 6G networks,” *IEEE Open J. Commun. Soc.*, vol. 2, pp. 1901–1914, 2021.

[174] M. Giordani and M. Zorzi, “Non-terrestrial networks in the 6G era: Challenges and opportunities,” *IEEE Netw.*, vol. 35, no. 2, pp. 244–251, Mar./Apr. 2020.

[175] F. Rinaldi *et al.*, “Non-terrestrial networks in 5G & beyond: A survey,” *IEEE Access*, vol. 8, pp. 165178–165200, 2020.

[176] B. Li, Z. Fei, C. Zhou, and Y. Zhang, “Physical-layer security in space information networks: A survey,” *IEEE Internet Things J.*, vol. 7, no. 1, pp. 33–52, Jan. 2020.

[177] X. Zhang, B. Zhang, and D. Guo, “Physical layer secure transmission based on fast dual polarization hopping in fixed satellite communication,” *IEEE Access*, vol. 5, pp. 11782–11790, 2017.

[178] G. Giambene, S. Kota, and P. Pillai, “Satellite-5G integration: A network perspective,” *IEEE Netw.*, vol. 32, no. 5, pp. 25–31, Sep./Oct. 2018.

[179] K. Guo, K. An, B. Zhang, Y. Huang, and D. Guo, “Physical layer security for hybrid satellite terrestrial relay networks with joint relay selection and user scheduling,” *IEEE Access*, vol. 6, pp. 55815–55827, 2018.

[180] V. Bankey and P. K. Upadhyay, “Physical layer security of multiuser multirelay hybrid satellite-terrestrial relay networks,” *IEEE Trans. Veh. Technol.*, vol. 68, no. 3, pp. 2488–2501, Mar. 2019.

[181] G. J. Sutton *et al.*, “Enabling technologies for ultra-reliable and low latency communications: From PHY and MAC layer perspectives,” *IEEE Commun. Surv. Tut.*, vol. 21, no. 3, pp. 2488–2524, Jul.–Sep. 2019.

[182] H. Ren, C. Pan, Y. Deng, M. Elkashlan, and A. Nallanathan, “Resource allocation for secure URLLC in mission-critical IoT scenarios,” *IEEE Trans. Commun.*, vol. 68, no. 9, pp. 5793–5807, Sep. 2020.

[183] B. Soret, P. Mogensen, K. I. Pedersen, and M. C. Aguayo-Torres, “Fundamental tradeoffs among reliability, latency and throughput in cellular networks,” in *Proc. Globecom Workshops*, 2014, pp. 1391–1396.

[184] W. Yang, R. F. Schaefer, and H. V. Poor, “Secrecy-reliability tradeoff for semi-deterministic wiretap channels at finite blocklength,” *Int. Symp. Inf. Theory*, 2017, pp. 2133–2137.

[185] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, “A survey on security and privacy issues in Internet-of-Things,” *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1250–1258, Oct. 2017.

[186] L. Sun and Q. Du, “A review of physical layer security techniques for Internet of Things: Challenges and solutions,” *Entropy*, vol. 20, no. 10, 2018, Art. no. 730.

[187] 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. Surv. Tut.*, vol. 16, no. 3, pp. 1550–1573, Jul.–Sep. 2014.

[188] D. Marabissi, L. Mucchi, and S. Morosi, “User-cell association for security and energy efficiency in ultra-dense heterogeneous networks,” *Sensors*, vol. 21, no. 2, 2021, Art. no. 508.

[189] X. He, R. Jin, and H. Dai, “Physical-layer assisted secure offloading in mobile-edge computing,” *IEEE Trans. Wireless Commun.*, vol. 19, no. 6, pp. 4054–4066, Jun. 2020.

[190] R.-F. Liao *et al.*, “Security enhancement for mobile edge computing through physical layer authentication,” *IEEE Access*, vol. 7, pp. 116390–116401, 2019.

[191] Z. Lu, G. Qu, and Z. Liu, “A survey on recent advances in vehicular network security, trust, and privacy,” *IEEE Trans. Intell. Transp. Syst.*, vol. 20, no. 2, pp. 760–776, Feb. 2019.

[192] V. Marojevic, “C-V2X security requirements and procedures: Survey and research directions,” 2018, *arXiv:1807.09338*.

[193] B. M. ElHalawany, A. A. A. El-Banna, and K. Wu, “Physical-layer security and privacy for vehicle-to-everything,” *IEEE Commun. Mag.*, vol. 57, no. 10, pp. 84–90, Oct. 2019.

[194] X. Luo, Y. Liu, H.-H. Chen, and Q. Guo, “Physical layer security in intelligently connected vehicle networks,” *IEEE Netw.*, vol. 34, no. 5, pp. 232–239, Sep./ Oct. 2020.

[195] Y. E. Sagduyu, T. Erpek, and Y. Shi, “Adversarial machine learning for 5G communications security,” in *Game Theory and Machine Learning for Cyber Security*. Hoboken, NJ, USA: Wiley, 2021, pp. 270–288.

[196] N. Papernot, P. McDaniel, X. Wu, S. Jha, and A. Swami, “Distillation as a defense to adversarial perturbations against deep neural networks,” *Symp. Secur. Privacy*, 2016, pp. 582–597.

[197] X. Cao and N. Z. Gong, “Mitigating evasion attacks to deep neural networks via region-based classification,” in *Proc. 33rd Annu. Comput. Secur. Appl. Conf.*, 2017, pp. 278–287.

[198] W. Guo, “Explainable artificial intelligence for 6G: Improving trust between human and machine,” *IEEE Commun. Mag.*, vol. 58, no. 6, pp. 39–45, Jun. 2020.

[199] D. Doran, S. Schulz, and T. R. Besold, “What does explainable AI really mean? A new conceptualization of perspectives,” 2017, *arXiv:1710.00794*.

[200] G. Thamilarasu and R Sridhar, “Exploring cross-layer techniques for security: Challenges and opportunities in wireless networks,” in *Mil. Commun. Conf.*, 2007, pp. 1–6.

[201] J. M. Hamamreh, M. Yusuf, T. Baykas, and H. Arslan, “Cross MAC/PHY layer security design using ARQ with MRC and adaptive modulation,” in *Wireless Commun. Netw. Conf.*, 2016, pp. 1–7.

[202] L. Zhou, D. Wu, B. Zheng, and M. Guizani, “Joint physical-application layer security for wireless multimedia delivery,” *IEEE Commun. Mag.*, vol. 52, no. 3, pp. 66–72, Mar. 2014.

[203] M. H. Johnson and W. K. Harrison, “A rateless approach to physical-layer security,” in *Int. Conf. Commun.*, 2018, pp. 1–6.

[204] B. Van Nguyen, H. Jung, and K. Kim, “Physical layer security schemes for full-duplex cooperative systems: State of the art and beyond,” *IEEE Commun. Mag.*, vol. 56, no. 11, pp. 131–137, Nov. 2018.

[205] J. Wu and P. Fan, “A survey on high mobility wireless communications: Challenges, opportunities and solutions,” *IEEE Access*, vol. 4, pp. 450–476, 2016.

[206] E. Güvenkaya, J. M. Hamamreh, and H. Arslan, “On physical-layer concepts and metrics in secure signal transmission,” *Phys. Commun.*, vol. 25, pp. 14–25, 2017.

[207] L. Mucchi, L. Ronga, X. Zhou, K. Huang, Y. Chen, and R. Wang, “A new metric for measuring the security of an environment: The secrecy pressure,” *IEEE Trans. Wireless Commun.*, vol. 16, no. 5, pp. 3416–3430, May 2017.

[208] K. S. Ryland, “Software-defined radio implementation of two physical layer security techniques,” Ph.D. dissertation, Virginia Tech, Blacksburg, VA, USA, 2018.

[209] S. A. Hoseini, F. Bouhafs, and F. den Hartog, “A practical implementation of physical layer security in wireless networks,” in *Proc. 19th Annu. Consum. Commun. Netw. Conf.*, 2022, pp. 1–4.

[210] F. Bouhafs *et al.*, “Wi-5: A programming architecture for unlicensed frequency bands,” *IEEE Commun. Mag.*, vol. 56, no. 12, pp. 178–185, Dec. 2018.

MUHAMMAD SOHAIB J. SOLAIJA (Student Member, IEEE) received the B.E and M.Sc degrees in electrical engineering from the National University of Science and Technology, Islamabad, Pakistan, in 2014 and 2017, respectively. He is currently working toward the Ph.D. degree with Istanbul Medipol University, Istanbul, Turkey, as a member of the Communications, Signal Processing, and Networking Center (CoSiNC). His research interests include interference modeling and coordinated multipoint implementation for 5G and beyond wireless systems.

HANADI SALMAN (Student Member, IEEE) received the B.S. degree in telecommunication engineering from An-Najah National University, Nablus, Palestine, in 2017. She is currently working toward the Ph.D. degree with Istanbul Medipol University, Istanbul, Turkey, as a member of the Communications, Signal Processing, and Networking Center (CoSiNC). Her research focuses on interference mitigation, resource scheduling, and coordinated multipoint (CoMP) for 5G and beyond wireless systems.

HÜSEYIN ARSLAN (Fellow, IEEE) received the B.S. degree from Middle East Technical University, Ankara, Turkey, in 1992, the M.S. and Ph.D. degrees from Southern Methodist University, Dallas, TX, USA, in 1994 and 1998, respectively.

From January 1998 to August 2002, he was with the Research Group of Ericsson, where he was involved with several projects related to 2G and 3G wireless communication systems. Between August 2002 and 2022, he was a Professor with the Department of Electrical Engineering, University of South Florida, Tampa, FL, USA. In December 2013, he joined Istanbul Medipol University, Istanbul, Turkey, to found the Engineering College, where he has been the Dean of the School of Engineering and Natural Sciences. He was also a part-time consultant for various companies and institutions, including Anritsu Company and The Scientific and Technological Research Council of Turkey. He conducts research in wireless systems, with emphasis on the physical and medium access layers of communications. His current research interests include 6G and beyond radio access technologies, physical layer security, interference management (avoidance, awareness, and cancellation), cognitive radio, multicarrier wireless technologies (beyond OFDM), dynamic spectrum access, co-existence issues, non-terrestial communications (high altitude platforms), joint radar (sensing) and communication designs. He has been collaborating extensively with key national and international industrial partners and his research has generated significant interest in companies, such as InterDigital, Anritsu, NTT DoCoMo, Raytheon, Honeywell, and Keysight technologies. Collaborations and feedback from industry partners has significantly influenced his research. In addition to his research activities, he has also contributed to wireless communication education. He has integrated the outcomes of his research into education, which lead him to develop a number of courses at the University of South Florida and Istanbul Medipol University. He has developed a unique Wireless Systems Laboratory course (funded by the National Science Foundation and Keysight Technologies) where he was able to teach not only the theory but also the practical aspects of wireless communication system with the most contemporary test and measurement equipment.

Dr. Arslan was the general chair, technical program committee chair, session and symposium organizer, workshop chair, and technical program committee member in several IEEE conferences. He is currently a member of the editorial board for the IEEE Surveys and Tutorials and *Sensors Journal*. He was also a member of the Editorial Board of the IEEE TRANSACTIONS ON COMMUNICATIONS, IEEE TRANSACTIONS ON COGNITIVE COMMUNICATIONS AND NETWORKING(TCCN), and several other scholarly journals by Elsevier, Hindawi, and Wiley Publishing. He is also an IEEE Distinguished Lecturer and a Member of the Turkish Academy of Sciences.