Received 4 June 2021; revised 9 July 2021; accepted 4 August 2021. Date of publication 10 August 2021; date of current version 17 August 2021.

Digital Object Identifier 10.1109/OJCOMS.2021.3103735

Physical-Layer Security in 6G Networks

LORENZO MUCCHI [1] (Senior Member, IEEE), SARA JAYOUSI[1], STEFANO CAPUTO[1], ERDAL PANAYIRCI [2] (Life Fellow, IEEE), SHAHRIAR SHAHABUDDIN [3] (Member, IEEE), JONATHAN BECHTOLD[4], IVÁN MORALES[5], RAZVAN-ANDREI STOICA[4], GIUSEPPE ABREU [5] (Senior Member, IEEE), AND HARALD HAAS [6] (Fellow, IEEE)

[1]Department of Information Engineering, University of Florence, 50139 Firenze, Italy

[2]Department of Electrical and Electronics Engineering, Kadir Has University, 3408 Istanbul, Turkey

[3]Nokia Mobile Networks, 90650 Oulu, Finland.
[4]WIOQnet GmbH, 28717 Bremen, Germany

[5]Department of Electrical Engineering and Computer Science, Jacobs University Bremen, 28759 Bremen, Germany

[6]LiFi Research and Development Centre, Department of Electronic and Electrical Engineering, University of Strathclyde, Glasgow G1 1XW, U.K.

CORRESPONDING AUTHOR: L. MUCCHI (e-mail: lorenzo.mucchi@unifi.it)

This work was supported in part by the European Union's Horizon 2020 Research and Innovation Programme under Grant 872752; in part by the European Telecommunications Standard Institute (ETSI) SmartBAN; in part by the Technical and Research Council of Turkey (TUBITAK) through the 1003-Priority Areas Project under Grant 218E034; in part by the Academy of Finland 6Genesis Flagship under Grant 318927; in part by the by COST (European Cooperation in Science and Technology) through COST Action NEWFOCUS; and in part by the EPSRC Established Career Fellowship Grant EP/R007101/1.

ABSTRACT The sixth generation (6G) of mobile network will be composed by different nodes, from macro-devices (satellite) to nano-devices (sensors inside the human body), providing a full connectivity fabric all around us. These heterogeneous nodes constitute an ultra dense network managing tons of information, often very sensitive. To trust the services provided by such network, security is a mandatory feature by design. In this scenario, physical-layer security (PLS) can act as a first line of defense, providing security even to low-resourced nodes in different environments. This paper discusses challenges, solutions and visions of PLS in beyond-5G networks.

INDEX TERMS 6G, physical-layer security, MIMO, IRS, visible light communications, authentication, key distribution.

I. INTRODUCTION

THE 6TH GENERATION (6G) communication networks are portrayed to form a full connectivity fabric, with a high degree of operational flexibility and autonomy [1], [2]. The network nodes may furthermore span from satellite links to intra-body communications, while the core traffic is expected to still be undertaken by what is traditionally known as the cellular network that 5G still deploys.

The distributed thinking paradigm taken to the core of the radio heads and network deployment sparkled thus far by 5G will only intensify with the upcoming technologies beyond 5G (B5G) (e.g., cell-free multiple-input multiple-output (MIMO), intelligent reflective surfaces (IRS) and self-aggregating networks, predictive resource management & link processing, *etc.*). The new services and value-added propositions of mobile edge computing, but also the growing requirements of "infinite-like" connectivity as well as the decreased link/end-to-end latency requirements of a pervasive context-aware next-generation Internet, will motivate the B5G technologies deployment.

These advanced holistic network functions are expected to be researched and implemented based on optimized, distributed and autonomously established communication links under new access schemes and network protocols leveraging upcoming trends of machine learning (ML) and artificial intelligence (AI), but also modern signal processing techniques (e.g., matrix completion, random finite matrix algebra, compressive sensing or simulated annealing). Under this disruptive connectivity paradigm, attack vectors will naturally increase exponentially.

Furthermore, the advances of quantum computing enabling quantum processing and search algorithms (e.g., Grover's algorithm, Shor's algorithm [3]) will similarly contribute and widen the latter threat surface. The progress in this area of computing will inadvertently exploit the discrete logarithm problem that current cryptographic mechanisms such as elliptic-curve cryptography, Diffie-Hellman key exchange (DHKE), elliptic-curve Diffie-Hellman (ECDH) protocol, transport layer security (TLS) / datagram transport layer security (DTLS) heavily rely on [4]. As a result, if not post-quantum amended, the latter security protocols are expected to be rendered obsolete, and so, deprecated for secure usage in B5G and 6th generation (6G) networks [4].

Within these expectations, the security of ultra-dense networks of heterogeneous nodes becomes paramount to provide truly scalable, adaptive, quantum-safe security solutions towards 6G connectivity. These aspects motivate a bottom-up approach in leveraging all the available security planes over the generic communication stack, and to this end, one key candidate technology is the PLS [5]. PLS has been often forgotten in this context of security, despite its intrinsic contextual and entropic richness. 5G implementation does not include PLS technology, keeping still commercially unexplored the potentiality of the security at physical layer. This status quo needs not to continue and in the context of B5G should be disrupted to opportunistically leverage the available secrecy capacity and universally secure the communication links at low costs as needed. Therefore 6G should implement PLS to cope with the new security challenges derived from advanced application scenarios (e.g., ultra dense heterogeneous networks characterized by different capable devices with multiple mobility levels). Abstractly, PLS can be reduced to an advantage for system designers who may use the physical model and environment to gain a security advantage over active and passive attackers [6]. In terms of communication systems, these advantages are plenty and rely heavily on the channel propagation models, channel reciprocity characteristics, spatial diversity, antenna diversity, geometric and positional secrecy, cooperative beamforming/jamming *etc.*, as illustrated in Fig. 1.

Thus, all of these may be embedded into future protocols to create secure by design communication links, even for very low complex devices/networks. The physical layer in 6G will play an important role to support higher bandwidths, higher carriers, lower latencies, all with lower energy consumption. Security cannot be left apart, and should be a basic key performance indicator (KPI) of future wireless networks. This paper discusses how 6G can benefit from the use of PLS.

Before evaluating the state of the art, it is important to point out that all the PLS techniques can be applied to 5G and 6G indifferently. From PLS point of view, anyway, there are differences between 5G and 6G. In particular, 6G foresees a deeper integration of heterogeneous networks, from nano-devices into the body to high altitude platforms or satellites. If 5G will enable the IoT paradigm, 6G is envisioned to speed it up and to give it uniform performance anytime anywhere any-device any-environment (land, sea, air, space, etc.). To address security in such a high heterogeneous network, plenty of data coming from devices with high heterogeneous resource capabilities, PLS is envisioned to be a high important technique to assure an uniform security level all over the network.

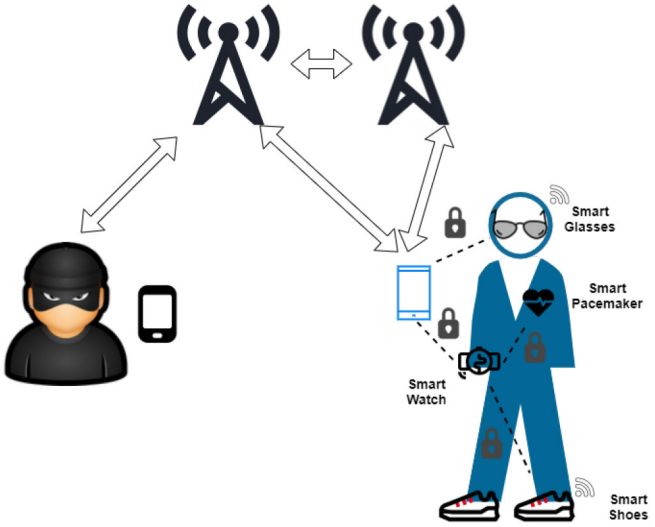

FIGURE 1. 6G needs to solve unprecedented security threats.

A. STATE OF THE ART ON PHYSICAL-LAYER SECURITY

The history of PLS is long. From early '50s when Shannon studied the concept of perfect secrecy to '70s when Wyner derived the role of channel noise (randomization source) in providing security. After that period, there was a long interval without publications on PLS, due to the unpractical implementation of PLS to real communication networks. The situation changed in the first decade of XXI century, when the wireless networks started to spread around. Advances in multi-antenna systems, adaptive coding and signal processing have brought new possibilities to design asymmetries in channel quality between legitimate and enemy nodes.

Wide acceptance of PLS as a concrete security mechanism is still ongoing, but surely PLS is recognized as an additional level of security, complementary to cryptography. While the security level of cryptography depends on the (limited) computational power of the enemy, PLS assumes an asymmetry in signal quality reception by legitimate and enemy nodes.

Many tutorial papers have been published on PLS, whose main representative ones are the followings: [8], [9], [10], [11], [12], [13], [14], [15], [16], [17], [18], [19], [20], [27]. In [9], fundamentals of PLS are given, as well as a vision on PLS in single- and multi-antenna, multiuser and relay systems. In [10], a comprehensive overview of security threats in wireless communications is given for different layers, including PLS. In [11], an overview of PLS for user authentication and device identification is provided. In [12], PLS is foreseen to provide handover security for

heterogeneous 5G networks. In [13], challenges and opportunities on the use of physical-layer parameters to obtain device fingerprinting are given. An overview of threats and challenges in cyber-security can be found in [14], while an overview of PLS techniques and applications can be found in [15]. The use of PLS for authentication is discussed in [16], including real implementation difficulties. An overview of PLS techniques with imperfect channel information is given in [17]. A review of applications of PLS to the Internet of Things (IoT) context is given in [18]. An overview of multiple input multiple output (MIMO) techniques for PLS is in [18], while [19], [20] provide a review of error-coding for PLS. The issue of active eavesdropper or multiple eavesdroppers in heterogeneous networks is addressed in [21], [22], [23], [24], while the issue of pilot spoofing in MIMO systems is considered in [25], [26]. In [27] an overview of PLS techniques is discussed, including open research points and future directions in next generation wireless networks.

The PLS approaches can be then categorized using the following classes:

- *Secrecy rate:* The maximum transmission rate at which the eavesdropper is unable to recover any information about the message by analysing the received signal. any technique which produces a signal-noise-ratio (SNR) advantage over the eavesdropper increases this rate. Main general drawback: it requires to know the position of the eavesdropper.
- *Physical Authentication:* The reciprocity of the legitimate wireless link is exploited to produce a common shared secret. This approach can be used to let the legitimate nodes extract a (common) cipher key by analysing the channel. In general, PLS authentication techniques can exploit randomnesses of the wireless channel in time, in frequency and in space domains [15].
- *Beamforming:* Use of multiple directional antennas to randomize the transmitted information stream or to inject noise in the direction of the eavesdropper. Main general drawbacks: it requires to know the position of the attacker; it increases the interference over other legitimate links.
- *Spectrum spreading:* One of the most used technique is the hopping of the signal over multiple frequencies, following a pre-determined sequence, like in Frequency Hopping Spread Spectrum (FHSS). Main general drawbacks; the cipher sequence has to be known in advance and thus shared over a secure channel. It is important to highlight that the FHSS is not usually inserted in the PLS-based techniques in literature. Anyway, it actually acts at the physical-layer.
- *Cooperation:* Friendly nodes send noisy signals towards the eavesdropper in order to deteriorate its link. Main general drawbacks: it requires to know the position of the eavesdropper; it increases the interference of the system; more energy is needed to provide security of a single link.

B. OUR CONTRIBUTION

Despite the huge amount of papers published on PLS, including tutorials and overviews, there is no paper which provides a specific vision of the application of PLS in 6G.

Abstractly, PLS can thus be reduced to any advantage system designers may take of the physical model and environment to gain a security advantage over active and passive attackers [6]. In terms of communication systems, these advantages are plenty and rely heavily on the channel propagation models, channel reciprocity characteristics, spatial diversity, antenna diversity, geometric and positional secrecy, cooperative beamforming/jamming *etc.*, as illustrated in Fig. 1. Thus, all of these may be embedded into future protocols to create security by design communication links, even for very low complex devices/networks. The physical layer in 6G will play an important role to support higher bandwidths, higher carriers, lower latencies, all with lower energy consumption.

PLS is the first line of defense, and it can provide security even to low complex nodes in different scenarios. This paper discusses about the challenges, solutions and visions of PLS in beyond-5G systems from several aspects.

The remaining sections are organized as follows. Section II introduces the security requirements and threats in 6G networks, while Section III highlights the possible implementations of PLS. Section IV concludes the paper and gives future directions.

II. SECURITY REQUIREMENTS AND THREATS IN 6G NETWORKS

A. SECURITY THREATS IN 6G NETWORKS

6G is envisioned as a hyper-connected fabric surrounding hyper-dense networks of heterogeneous nodes. This revolutionary feature asks for hyper-security, since (personal) data is acquired anytime-anywhere seamlessly, even from small objects (a bottle of water, etc.) individuals interact with. 6G has thus to be designed as a network with embedded trust in Internet of Everything (IoE) and artificial intelligence (AI) era. Both data acquisition points and computational points in the overall network will be largely distributed. 6G network should not only provide efficient and usable services, but also secure. This implies that all the astonished KPIs of 6G should be considered taking into account that all services must comply with security and privacy requirements. Specifically, security questions in 6G networks are:

- how threats can be detected in ultra-dense heterogeneous networks with different levels of nodes complexity?
- how confidentiality and integrity can be maintained without decreasing the user's experience?
- how same level of security can be assured over multiple trust domains?
- how security can be met in dense networks composed by millions of very low complex devices?
- will the extensive use of AI-based networks open the door to new threats?

- pushing intelligence towards the edge of the network will open additional security threats?

In this context, stronger protection can be achieved by implementing security at the physical layer. Integrating physical layer with cybersecurity is the key to face security challenges of future 6G networks. An overview of security and privacy threats and challenges in 6G networks can be found in [28].

B. PLS TECHNIQUES

PLS provides security at the very first layer (physical), acting as a first line of defense, trying to make attackers' job harder. It provides confidentiality without assuming a limited computational power of the hostile node, by exploiting unique characteristics of the wireless channel. In the quantum computing and AI era applied to networks, it is important not to rely on unfair assumptions about the attackers for providing security.

Some of the main PLS techniques consist of: i) signal processing (noisy modulations); ii) coding (wiretap codes); iii) artificial noise injection (friendly/cooperative jamming); iv) MIMO/IRS (beamforming destructive signal); v) HetNets (user/BS association to provide larger area of security); vi) visible light communications (VLC) (spatial confinement of signals) and vii) cipher-Key generation.

An overview of PLS techniques and applications is provided by [15].

C. PLS IN 6G SCENARIOS

In order to highlight what PLS can do for 6G and how the previously listed PLS techniques can be mapped into different application contexts, four main scenarios are defined:

1. *Low-resourced devices:* It includes both dry and wet nano-scale devices and the adoption of signal processing and coding PLS techniques represent a promising solution to be considered. Dry and wet devices refer to biological or artificial nano-scale machines. For example, synthetic biology can design and implement biological particles (wet) to interact with the natural cells following a programmed plan. Similarly, artificial nano-scale robots (dry) can be designed to provide actions inside the human body.
2. *Massive deployed devices with mobility:* The exploitation of Massive Cell-Free MIMO and Intelligent reflecting surfaces (IRS) shall be taken into account to satisfy the security requirements of such context.
3. *Indoor environments:* The spatial confinement that visible light communications offers can be very useful to guarantee indoor secure communications.
4. *Opportunistic/self-organizing networks:* Fast generation of PhySec-based crypto-key for symmetric encryption can represent a completely decentralized solution for key creation.
5. *Integrated sensing and communication:* Radar as well as high-resolution localization capabilities will be one key feature of the future mobile communication network. Understand the surrounding situation and localize precisely the users is a key-enabler of future 6G services, but on the other hand it opens new security issues, since sensing can also be target of attacks, and it can be the way to distort the communication. PLS can be very helpful in the protection of the sensing capabilities of 6G nodes.
6. *Edge computing and learning:* The data from users will be more and more computed as nearest as possible to the users, which produce and consume data/information. The edge computing together with federated learning technique will be an enabler of future 6G wireless services for mobile users, but this opens also new security threats: malicious end-user devices can attack edge node or provide adversarial training which could distort the learning model. PLS can be one important actor in protecting the edge nodes as well as the user equipment by exploiting features such as the fingerprinting authentication or the fast cipher key generation by means of channel reciprocity.

III. IMPLEMENTATIONS OF PLS

In this section examples of implementation of PLS are illustrated.

A. PLS FOR LOW-RESOURCED DEVICES

Many of the approaches described in Section I are based on assumptions that make them not easily implementable in a real world: some of those require that a common a priori secret is shared by the legitimate users or exchanged in the start-up phase through insecure channels, and some others assume to know that an eavesdropper is present and where it is located. As a matter of fact, almost all existing results on secret channel capacity are based on some kinds of assumptions that appear impractical. It has been a challenge in information theory for decades to find practical ways to realize information-theoretic secrecy.

First proposals deal with the exploitation of the wireless channel between legitimate users in order to extract a key to be used for encrypting the message [29]. The information-theoretical secrecy ensures that if the extraction is made under the assumption to have an advantage over Eve's channel, the key is not recoverable by Eve in any way. An exhaustive review of cross-layer techniques for enhancing the security can be found in [29]. In [30], the security issues and solutions are reviewed for what concerns the IoT topic area. The physical-layer security anyway is not taken into account as information-theoretical secrecy. An overview of the challenges facing physical-layer security is reported in [31]. A review of cooperative techniques for enhancing the security can be found in [32].

Moving beyond the 5G technology, 6G will enhance the key performance indicators of 5G, enabling the definition of more demanding applications, ranging from augmented

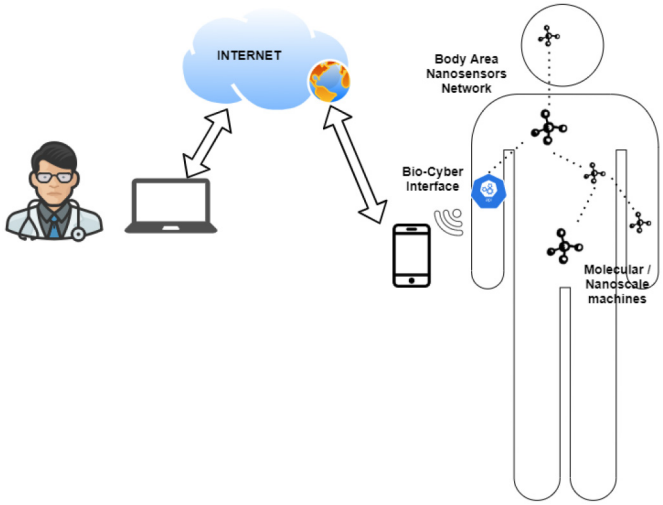

FIGURE 2. Human body as part of the global network.

reality and holographic projection to ultra-sensitive applications. In this context, a holistic approach of security is required to cope with the plethora of different systems and platforms. The large amount of the world data collected by networks of sensors (environmental, human-body, etc.) and the mobility features of most scenarios ask for advanced security techniques that take into account new constraints in terms of device capabilities, network environment and network dynamic topology [33]. PLS, moving the security strategy at physical layer, might be one of the confidentiality enablers in 6G connectivity. Its features, combined with the advances in artificial intelligence algorithms and the trend of distributed computing architectures, can be exploited either to enhance the classical cryptographic techniques or to meet the security requirements when dealing with simple but sensitive devices which are unable to implement cryptographic methods, e.g., devices and nano-devices of the Internet of Things and bio-nano-things where the human inner bodies become nodes of the future Internet [5] (Fig. 2).

Computational and energy resources of a network node can be reduced by adapting the security algorithm to the environmental context where the communication occurs, leading to the definition of a context-aware security approach. The dynamic context in terms of mobility, network nodes density, frequency spectrum utilization and technology heterogeneity which is envisaged in 6G scenarios should be taken into account in the definition of security communication strategies both for the identification of the level of security countermeasure needed in a specific moment and for the exploitation of these environmental characteristics in the security algorithm definition. Environmental and operational intelligent physical layer security also based on the adoption of AI algorithms may lead to a the definition of new techniques that can early detect the need of enhanced security mechanism to be dynamically activated (e.g., based on the battery level of the involved devices or the degree of trustworthiness of the specific context) and do not considerably affect the transmission spectral efficiency [34]. This approach complies with the main 6G key features that the enabling communication technologies should meet in term of low energy consumption and long battery life, high affordability and full customization and distributed artificial intelligence architectures. It is worth mentioning that ETSI SmartBAN group is working on the standardization of security and privacy for the future body area networks, and physical layer security is one candidate to handle the confidentiality of in- and on-body devices with typically low resources available. This is important also when 6G will include in- or on-body nodes as part of the Network (Fig. 2).

Physical layer security addresses one of the most important application of 6G: the human-centric mobile communications. In this framework, an increasing interest of scientific research has been oriented to wireless body area network and in particular to on-body and in-body nano-devices, including biochemical communications. In the next future, the human body will be part of the network architectures, it will be seen as a node of the network or a set of nodes (wearable devices, implantable sensors, nano-devices, etc.) that collect sensitive information to be exchanged for multiple purposes (e.g., health, statistics, safety, etc.). By coping with the high security and privacy requirements and the energy and miniaturization constraints of the new communication terminals, the Physical layer security techniques can represent efficient solutions for securing the most critical and less investigated network segments which are the ones between the body sensors and a sink or a hub node.

Two interesting potential application scenarios for physical layer security in 6G context are Human Bond Communication [35] and Molecular Communication [36]. The former requires a secure transmission of all the five human senses for replicating human biological features, allowing disease diagnosis, emotion detection, biological characteristics gathering and human body remote interaction. While the latter, based on the shifting of the information theory concepts in the biochemical domain (communications among biological cells inside the human body) requires advanced low-complexity and reliable mechanisms for securing intra-body communications and enabling trustworthy sensing and actuation in a challenging environment as the human body is (e.g., secure Internet of Bio-Nano Things) [36]. As en example of PLS applied to in-body communications with ultra-low complex devices, Fig. 3 shows two in-body nano-machine (e.g., particles) which communicate thought molecules diffusion. How to protect this link from nano-machine based eavesdropping? Secrecy capacity is defined as

$$C_s = \max\{0, C_B - C_E\} \tag{1}$$

where C_B and C_E is the capacity of Bob's and Eve's channel, respectively, and represents the maximum secure data rate that can be achieved over the legitimate communication link. Fig. 4 shows the secrecy capacity map of a communication between two legitimate particles through molecules diffusion.

Other recent interesting techniques, which do not rely on any knowledge about the attacker, spread from the use of

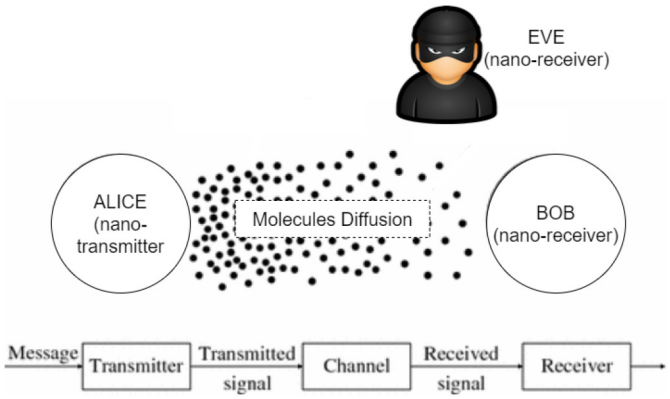

FIGURE 3. Molecular communications scheme with eavesdropper.

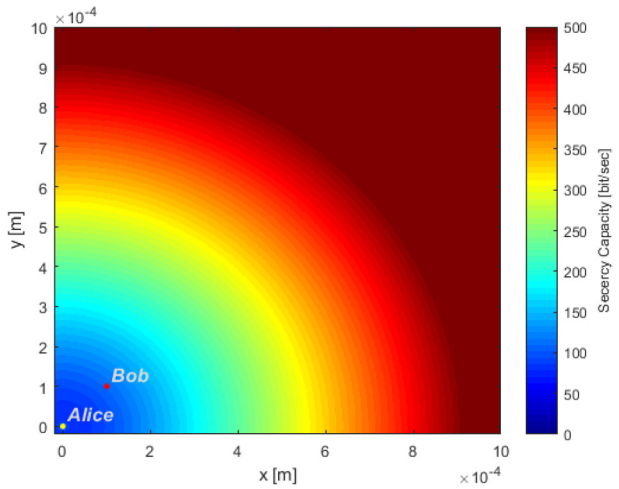

FIGURE 4. Secrecy capacity map of in-body particles communication thought molecules diffusion.

watermarking to the use of channel noise to modulate the information. In [37], the fading experienced by the channel between two legitimate nodes is used to dynamically create a common secret. In [38], game theory is used to jointly optimize the reliability and secrecy of legitimate nodes. In [39], a watermark is inserted into the host signal to produce security at physical layer. In [40], the thermal noise of the legitimate nodes is used to modulate the information exchanged. The latter is demonstrated to have an intrinsic unbreakable security, no matter the computational power or the position of the attacker is. Unfortunately, only low data rate can be supported (voice and text services).

B. DISTRIBUTED AND COOPERATIVE PLS PROTOCOLS

PLS can not only be used to provide keyless and innately secure communications by maximizing the secrecy rate, but also to co-generate cipher keys for symmetric encryption by exploiting the propagation characteristics of the wireless channel at the physical layer (PHY) layer. Transcending the provisioning of keyless and innately secure communication by secret rate maximization, PLS may also exploit the intrinsic physical propagation characteristics of the

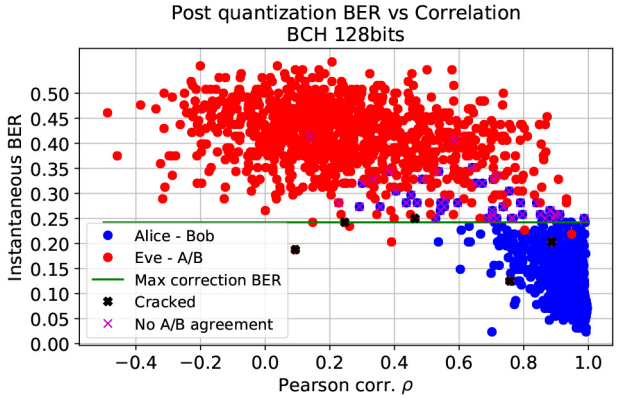

FIGURE 5. Secret Key Generation resilience against key sniffing.

wireless channel to co-generate cryptographic keys for symmetric encryption. This strategy is particularly useful for latency-constrained communications and resource-constrained radios, where the secrecy enhancing traditional techniques become impractical. This is usually the case for high device densities under opportunistic self-organizing network formation paradigms or upcoming autonomously communicating device-to-device (D2D) nodes. Opportunistic self-organizing networks as well as autonomous D2D communications are two example scenarios where the traditional security strategy cannot be easily applied.

Standardized encryption ciphers are often considered unassailable for data confidentiality and integrity since they are just deterministic mathematical operations that are as secure as the shared random secrets they rely on. Therefore, the main focus for the future ubiquitous wireless connectivity and digitization relates to authentication and key distribution. Which by the broadcast nature of wireless communications, are inherently vulnerable to eavesdropping, range extension and informational non-intrusive yet effective man-in-the-middle (MITM) attacks.

PHY-based key generation, compared to traditional solutions, is completely decentralized and does not rely on fixed parameters designed by a specific entity [6]. Instead, it uses the shared wireless channels as a distributed entropy source to arrive at a shared secret that is not directly dependent on deterministic operations. Preliminary results in Fig. 5 show that the shared wireless channel can be used as a distributed entropy source which is highly correlated between parties trying to establish a common secret, but is much less correlated for a malicious device trying to access this information. These results were generated using off-the-shelf MCUs communicating over a min latency Bluetooth Low Energy established connection, and two cooperating eavesdroppers with full knowledge of the key generation procedure and parameters were placed within half a wavelength of the generating parties respectively. Furthermore, this data is representative of static and dynamic scenarios where the distance between terminals changed with a rate matching that of a pedestrian, and produced 95% key agreement between terminals, with <1% of these keys being

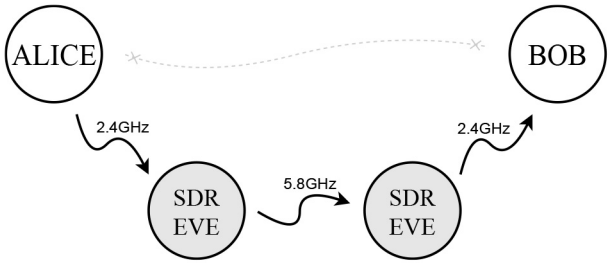

FIGURE 6. MITM tested scenario.

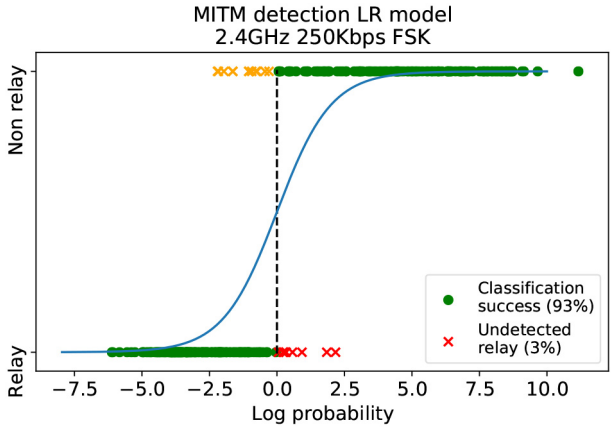

FIGURE 7. MITM detection using SDR as Amplify and Forward relays.

sniffed by the eavesdroppers. To capture this entropy towards key generation, channel sensing must be performed beyond the currently available radio channel metrics for application layer development.

In fact, with the advance of virtualization, it is expected that newly developed or existing communication protocol implementations should expose the PHY attributes from all exchanges, such as channel state information (CSI), received signal strength (RSSI), carrier frequency offset (CFO), *etc.*, to the upper logic layers of the communications system. As a result, such physical channel data will become widely available for analysis and encourage the development of PHY-based security and authentication solutions. In such a future, the wireless physical characteristics become the root of trust enabling data confidentiality, integrity and link level authentication. During this process, physically co-generated symmetric dynamic secrets will enhance the value of fast, resource-friendly symmetric ciphers, providing promising guarantees towards future perfect secrecy. Consequently, communication can become more resilience to existing DHKE vulnerabilities and the real-time (quantum) computing attacks [4].

These issues will become more prominent in future networks given the introduction of D2D communications in 3GPP Releases, which open the door to proximity-based services (ProSe) [41]. Coupling these services with the current trends towards autonomous intelligent nodes capable of cooperation will open new low-level attack vectors at the PHY-layer. Such vulnerabilities are exploitable by malicious relaying and proxying that can spoof distances between devices, like extension/reduction attacks. Contrary, to popular belief, encryption alone is not effective against low-level signal manipulations [7], as adopting more secure ciphers will not resolve the vulnerabilities in side channel attacks at the PHY-layer which don't try to compromise the system by directly interpreting or manipulating the transmitted data. An example of such a scenario is the MITM relay attack in Fig. 6, where a first eavesdropper captures the broadcasted signal, up-converts it to a faster channel for transmission over the air, and is then received, down-converted and rebroadcasted by a second eavesdropper node.

Classical signal processing techniques can be used to implement countermeasures, e.g., by identifying anomalies in the PHY attributes of the received signals or in the packet exchanges. However, resource-constrained devices require lightweight implementations of such techniques, which are not always viable. Therefore, ML is the true potential for threat detection, where massive amounts of high level physical attributes can be utilized to instruct ML models for pattern recognition, classification and monitoring. ML-based networks can exploit channel attributes to enable real-time PHY-monitoring and knowledge-based detection, leading AI companies to develop security-as-a-service (SecaaS) watchdogs. An example showing the potential of ML techniques for threat detection is seen in Fig. 7, where the classifier was trained to distinguish between a direct peer to peer communication scenario and the attack scenario displayed in Fig. 6, where off-the-shelf MCUs and the Bluetooth Low Energy PHY stack was leveraged. In this system, the legitimate transmitter modulates pilot signals broadcasted to the receiver to accentuate the channel effects introduced by the compound channel characteristic of a relay attack. The receiver then extracts a small set of features which in this case were used in a very simple Logistic Regression model, alternatively in the case of bidirectional communications, the same feature set can be extracted on both terminals and compared to assess the authenticity of the communication link.

The topology of the network will influence largely the deployment of SecaaS applications. For example, networks including nodes which actively route local packets can detect active threats by using the latter as physical aggregators. Similarly, an edge server (passive observer) with high computational power can enhance the embedded D2D threat real-time revealing capabilities of the network by acting as the aggregator of packets and PHY data in SecaaS applications.

The higher the number of diversified and independently generated threat revealing models at each aggregator/node, the larger the security paradigms that can eventually be extracted from these. Enabling transfer learning techniques to be developed depending on the diversity of such models. Allowing adjacent networks and subnetworks to share learned parameters between one another and better monitor and detect novel malicious attacks.

C. CELL-FREE MASSIVE MIMO AND IRS

The most successful PHY technology for 5G networks is massive MIMO. A massive MIMO base station (BS) supports a large number of antennas that cover a large number of terminals [42]. Massive MIMO technology is popular among network vendors due to their superior spectral efficiency and throughput. Network vendors adopted massive MIMO for pre-5G products which have been displayed on numerous trials in last few years. For example, Nokia and Sprint demonstrated massive MIMO with 64 antennas connected for both uplink and downlink through their AirScale products in Mobile World Congress (MWC) 2017. Ericsson and Huawei also have similar products for massive MIMO such as AIR 6468 and Huawei AAU, respectively. The research community have already shifted their focus on post-5G networks and PHY technologies that grabbed most attention for 6G are: 1) Cell-free massive MIMO and 2) IRS. They are currently the two strongest candidates for physical layer of sixth generation (6G) communication systems. Both are currently strong candidates for PLS in 6G networks.

1) CELL-FREE MASSIVE MIMO

The biggest drawback of conventional massive MIMO is their distance from users, which cause large variations of received signal strength between different users. Distance from users is the biggest drawback of conventional massive MIMO, since different users experience large variations of received signal strength. Typically, a bulky and expensive massive MIMO BS is placed in an elevated location to increase the cell radius and to cover a large number of users. The cell/coverage radius is usually increased by placing a bulky and expensive massive MIMO BS in an elevated location. Cell-free massive MIMO eliminates this drawback by having antennnas distributed among different locations. The baseband functionalities are performed by a centralized baseband processing unit which is connected to all the antennas through cables [43]. This concept was displayed by Ericsson at MWC 2019, where they developed antenna stripes as small as matchbox and can be integrated in an adhesive tape to place in any locations. Ericsson, at the MWC 2019, displayed this concept: a matchbox-size antenna stripes were integrated into an adhesive tape which can be placed in any location.

As cell-free systems are also based on large number of antenna systems, the cell-free systems are also inherently robust against passive eavesdropping [19]. Cell-free massive MIMO systems provide PLS for passive eavesdropping without any extra effort. However, the eavesdropper can pretend to be a legitimate user and launch an active attack by sending a pilot sequence of his own. This pilot contamination attack is more challenging for a cell-free systems, because an amount of pilot contamination pre-exists in a cell-free systems. In [44], the authors have shown with mathematical analysis and Monte-Carlo simulations that active pilot contamination attack can be severely detrimental for provisioning PLS in cell-free massive MIMO systems. They compared co-located massive MIMO and cell-free massive MIMO, and the results revealed that cell-free systems are less resilient to pilot contamination attacks than conventional massive MIMO systems.

The research on PLS for cell-free massive MIMO system is at a very early stage and the existing literature on this topic is scarce. In [45], the security aspects of the cell-free systems are studied. The authors consider the problem of maximizing achievable data rate of the attacked user. The corresponding problems of minimizing the power consumption subject to security constraints are also considered. In [46], a secure communication in multigroup multicasting cell-free systems with active spoofing attack is investigated. A distributed conjugate beamforming with normalized power constraint policy is exploited for downlink secure transmission. Similar works can also be found in [47], [48]. These papers propose PLS exploiting information theory and signal processing rather than traditional higher-layer cryptographic techniques.

The biggest security issue associated with a cell-free massive MIMO is the exposed location of the antennas. It is easier to get physical access to cell-free system through the exposed antennas and cables compared to a remotely located massive MIMO BS. Hence, it is easier to inject malicious software and configuration parameters by direct wiretapping. The attacker could change the configuration of beamforming parameters so that the antenna arrays focus their signals towards an unwanted user. This also enables a passive attacker to get access on user-specific keys, short-term session keys and authentication keys. The requirement of a cell-free system dictates that the fronthaul circuitry connected with the antenna stripes should be simple. It is not possible to accommodate sophisticated encryption methods between the fronthaul and baseband unit. Thus, if an antenna stripe is compromised, it is very challenging to provide data confidentiality of the baseband transmissions or receptions. The cell-free systems are also vulnerable to physical attacks due to their exposed location and miniature size. It is much easier to destroy antenna stripes and disrupt the communication of a cell-free system than a remotely located bulky massive MIMO BS. It is much harder to destroy a remotely located bulky massive MIMO BS than an antenna stripes, and thus disrupt the communication of a cell-free system.

2) INTELLIGENT REFLECTIVE SURFACE

Intelligent Reflective Surface (IRS) is novel concept which provides an alternative path of transmission and can be used to change amplitude, phase and frequency of incident signals [49], [50], [51]. IRS is a new technique providing alternative path of transmission by changing amplitude, phase and frequency of incident signals. It is particularly useful for high frequency communication which suffers from

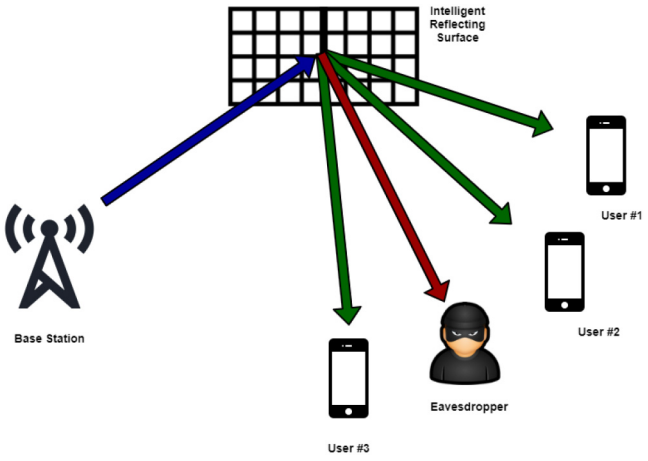

FIGURE 8. Intelligent reflecting surface (IRS) to produce security at physical layer.

high penetration and blockage loss. Instead of transmitting signal directly to an user, the signals are sent towards an IRS, which then reflects a beamformed signal towards a user (Fig. 8). Thus, IRS can be used to provide PLS by transmitting only towards a legitimate user through the alternative path [43], [52].

In [52], the authors investigated an IRS-aided secure wireless communication system where a multi-antenna access point (AP) sends confidential message in the presence of an eavesdropper. The authors solved an optimization problem which maximize the secrecy rate of the system by jointly designing AP's transmit beamforming and IRS's reflect beamforming. The authors demonstrated with simulation results that the IRS-aided communication system increased secrecy rate significantly by exploiting IRS-enabled power enhancement and interference suppression at the legitimate receiver and eavesdropper, respectively. Similar to [52], IRS-aided secure communication is also investigated in [53] and [54] for only one legitimate user and one eavesdropper with the aid of mathematical optimization. Secure IRS-based systems for multiple users and multiple eavesdroppers have been investigated in [55] and [56]. Both [55] and [56] enhanced the transmit beamforming by combining with a jamming or artificial noise. The reason is the transmitter lacks sufficient degrees of freedom when the number of users is smaller than the number of eavesdroppers. The authors verified with simulation results that the achievable secrecy rate is significantly higher with artificial noise injection with an IRS.

Despite the potential of IRS, the achievable secrecy rate is limited when the legitimate users and eavesdroppers have highly correlated links [52]. Therefore, IRS requires to constructively add beamformed signals towards the intended user and destructively add the towards eavesdropper. IRS has high security potential, but it requires that the signal towards the legitimate node must be beamformed constructively, while destructively towards the eavesdropper. Such signal processing techniques is not always trivial and it introduces additional complexity of the overall system. IRS requires to perform other signal processing techniques to track user location, estimate channel between user and IRS, and detect the incoming symbol vectors from the user. Without sophisticated algorithms, the signals can not be accurately beamformed towards intended user and the entire system becomes vulnerable to security threats. IRS platform security also has to be addressed for 6G PLS since attackers could physically access the IRS controller and modify configuration parameters. Finally, an attacker can place itself near the IRS and utilize the correlated channel to eavesdrop the incoming signals. Thus, it is of utmost importance to introduce mechanisms which can conceal the location of the IRS and its controller.

In a recent development, a variant of the IRS for full dimensional coverage is presented in [57]. A drawback of the IRS system is the legitimate users has to be located on the same side of the reflective surface and any user located on the opposite side of the metasurface is out of coverage. To address this issue, the authors presented intelligent omni-surfaces (IOS) in [57] with dual functionality of signal reflection and transmission. The IOS can reflect and transmit the incoming signals from one side towards mobile users of both sides, respectively. However, the achievable secrecy rate analysis of an IOS-based secure communication system remains an open problem.

D. PLS THROUGH OPTICAL WIRELESS COMMUNICATIONS

1) DEFINITION OF LIGHT-FIDELITY (LIFI)

The exponentially growth in mobile data traffic requires new spectrum in 6G. The optical spectrum offers three orders of magnitude more bandwidth than the entire radio frequency (RF) spectrum. Wireless networking with light is referred to as light-fidelity (LiFi) [58]. LiFi supports mobile devices that are randomly oriented. Seamless connectivity by means of handover and coordinated multipoint (CoMP) transmission, multiuser access, bi-directional communication are all functions that are supported in LiFi. The key difference to small cell RF communications is that the cells can get arbitrarily small giving rise to significantly improved area spectral efficiencies. The high density of LiFi access points requires a powerful backhaul which can be realized with optical wireless communication technologies.

Light as a data bearer offers attractive features such as high capacity, robustness to electromagnetic interference, a high degree of spatial signal confinement and controllability leading to inherent security features. LiFi can be used to build advanced wireless body area networks (WBANs), personal area networks (PANs), wireless local area networks (WLANs), vehicular area networks (VANETs) and it seamlessly blends into existing heterogeneous wireless networks. Light-based wireless communications will also enable the creation of wireless networks underwater where RF cannot be used except for ultra-short distances.

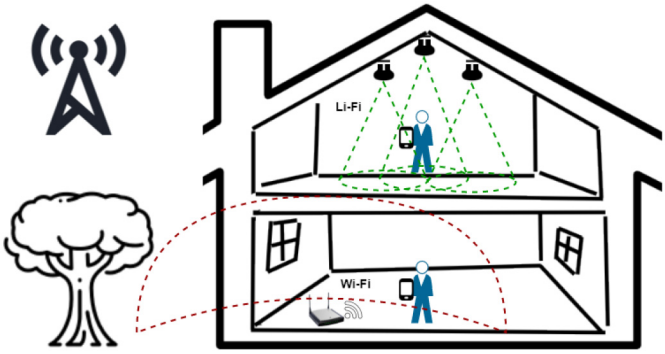

FIGURE 9. WiFi VS. LiFi. Light can confine the information where it belongs.

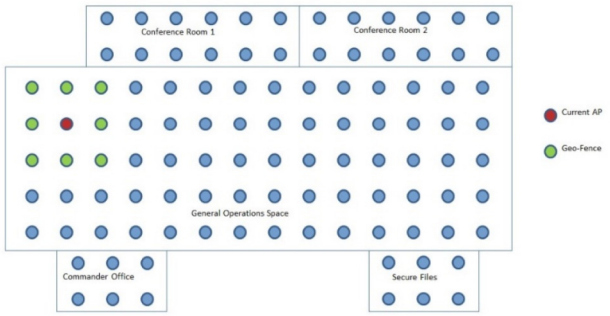

FIGURE 10. Network partitioning and physical layer security enhancements by exploiting signal confinements made possible by light as a data bearer.

2) UNIQUE OPPORTUNITIES FOR ENHANCE SECURITY THROUGH LIFI

PLS will play a vital role in enhancing cyber-security in wireless networks. Moreover, it will also help reduce both the latency and the complexity of novel security standards. The provision of user security is distributed across all layers of the open systems interconnect (OSI) model. The integrity and confidentiality of information is typically ensured by using secret and public key encryption methods. However, the strength of these techniques may be enhanced by reducing the attack surface. In this regard, the physical layer exposes significant vulnerabilities due to the broadcast nature of the wireless channel. It is well known that if the eavesdropper is equipped with sufficient computational power, protocol security can be compromised. Light does not propagate through opaque objects such as walls. It is also very directional – think of a laser beam in the extreme case. Hence, light beams can be formed without the need of excessive signal processing efforts. Lenses and other optical components can be used to shape a beam. It is, therefore, possible to significantly reduce the possibilities of man-in-middle attacks in LiFi compared to WiFi (Fig. 9).

On the other hand, fundamentals and techniques of PLS, developed for RF channels involving wire-tap coding, multi-antenna, relay- cooperation, and physical layer authentication, cannot be applied directly to VLC channels. This is mainly because many standard specifications in transmission protocols and modulation schemes of VLC systems are quite different from RF systems. Besides, light can easily be confined spatially and, since there is no fading because the wavelength is significantly smaller than the size of the detector, the VLC channels become more deterministic. These properties can be used for precise localization. All of these features of light can be harnessed to enhance security beyond PLS. For example, the movement patterns of users can be recorded. Subsequently, this data can be used to perform data analytics such as anomaly detection. LiFi allows orders of magnitude improvements in data density when compared to RF-based systems. It is possible to change access rights in such dense wireless networks almost at a centimeter precision level. Assume an office as shown in Fig. 10 which shows a typical floor plan of an office environment. There are rooms with different security levels. The network could be partitioned so that it is only possible, for example, to access the “secret files” wirelessly within the confined space of a secure file server room using special access rights. Anyone who would attempt to access secret information requires a) access to an account that has granted this these rights, and b) physical access to the secure file server room. This would be different if the wireless signals would propagate through the walls, in which case it would suffice to use account details that may have been acquired maliciously. The same principle could be used to create a “geofence" in any location. This means that a user would have standard account details such as “user name” and “password”, but in addition would have a ’location specific password’ - a second gate. This would then mean that access to the user’s account details would physically only be possible at the user’s current location (the serving access point is indicated with a red circle in Fig. 10.

For anyone outside the “geo-fenced" area access to users, the account would physically be impossible – even if they had maliciously acquired “user name” and “password". This means that man-in-the-middle attacks are substantially mitigated – if not eliminated.

In addition, MIMO and wavelength division multiplexing (WDM) can be employed to enhance physical layer security. In this context, spatial modulation (SM) exhibits advantageous features due to its property to use the propagation channel for information transmission. In SM, the information is carried by the transmitted symbols, as well as by the indices of an active transmit unit [58], [59]. It is important to note that SM-based MIMO transmission exploits the random switching among the antennas (LEDs) that generate a strong and friendly jamming signal, which is invaluable for PLS applications. MIMO and MIMO-SM-based physical layer security systems were studied extensively in research and development work widely presented in the literature. They are mostly based on techniques such as jamming, mapping of transmitted symbols, precoding, and subset selection, as well as combinations of these techniques. In particular, one of the precoding approaches, namely,

zero-forcing precoding (ZFP), is preferred widely in most applications due to its simplicity. Through the channel state information at the transmitter (CSIT) of the legitimate user, the precoding matrix coefficients are constructed through some optimization techniques so that the confidential message is perceived by the legitimate user clearly while the eavesdropper's bit error rate (BER) performance is degraded substantially [60], [61], [62], [63], [64]. On the other hand, a well-known method based on generating a friendly jamming signal creates an artificial noise, which lies in the null space of the legitimate user. After combining the confidential information with the jamming signal at the transmitter side, only the eavesdropper will experience destructive effects from the jamming signal [27], [65], [66], [67], [68]. The secrecy enhancement techniques, based on enhancing the secrecy rate by transmitting symbol mapping, the secrecy is realized by an encryption key for the given modulation. The same key is used at the legitimate user's side to decode the confidential message [62], [69], [70]. Another PLS enhancement technique, called *transmitter subset selection*, is based on choosing a specific subset of transmitting entities according to the radiation patterns of the transmitting units. The design of confidential signal sets is based on maximizing the minimum Euclidean distance or SNR at the legitimate user. Thus, it is clear that the eavesdropper's achievable performance would be lower than that of the legitimate user [71], [72], [73], [74].

Finally, the hybrid design of VLC and RF systems was expected to improve the user experience, substantially, since VLC systems can support reliable high data rates in specific areas and RF systems can provide coverage when a line-of-sight link is not available [75]. In Fig. 11 a hybrid VLC and RF system is illustrated. They can coexist, operating in the same environment, without causing any interference. It is also possible that both systems share the same physical layer techniques and medium access control (MAC) algorithms such as authentication and encryption. Recent transmission techniques such as spatial modulation (SM), spatial shift keying (SSK), OFDM-index modulation, transmitter precoding have been applied for PLS successfully in both optical and RF communications, separately. They have the capability reduce inter-channel interference while providing high power efficiency and detection simplicity. Recently, a new channel coding technique has been proposed to improve the error correcting capability by creating redundancy in the spatial domain [76]. In [60], [61], optical spatial constellation design techniques are presented with generalized space shift keying signaling for single-user and multi-user PLS where the received spatial constellations are optimized through a novel precoding scheme, which minimizes the BERs at legitimate users and significantly worsens eavesdroppers' BER. It has been shown that a similar PLS technique could also be employed in RF communications [77]. Relay-aided secure broadcasting for VLC was also investigated. A transmitter luminaire communicates with the legitimate receivers in the presence of an external eavesdropper [65], which can

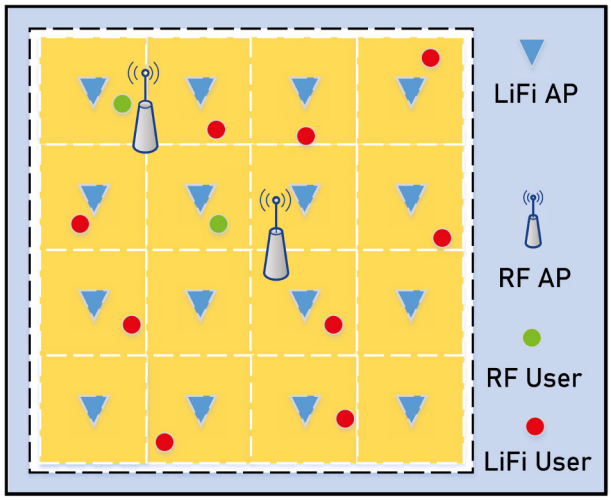

FIGURE 11. RF/optical wireless hybrid system model.

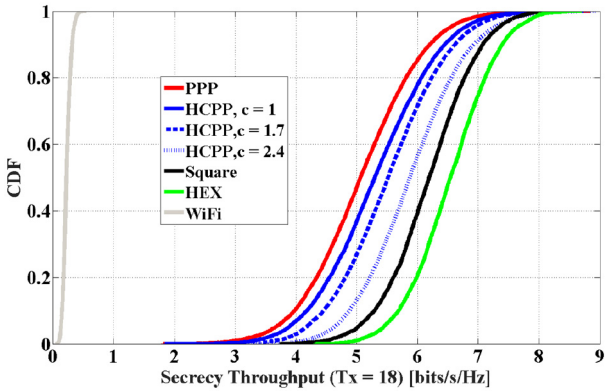

FIGURE 12. The CDF of WiFi and LiFi secrecy throughput. Four different types of LiFi deployment are evaluated: point Poisson process (PPP), Matérn hard core point process (HCPP), regular square topology, and regular hexagonal topology (HEX). The parameter *c* [m] denotes the minimum radius of the HCPP.

be combined for hybrid RF/Optical PLS systems. On the other hand, high quality of Service (QoS) is provided by the convergence of heterogeneous networks (HetNets). They usually involve different access technologies such as macrocell, microcell, femtocells, and attocell, consisting of RF and optical wireless-based networks [78], [79], [80]. Since hybrid VLC/RF systems have both VLC and RF components altogether in the system, physical layer security for such systems should be jointly investigated due to the broadcast nature of both technologies [81]. A recent survey paper [82], as well as in the literature specified therein, covers almost all aspects of PLS for VLC.

Fig. 12 shows a comparison between the secrecy throughput that can be achieved by WiFi and by LiFi in a 20×103 m room. The WiFi system uses a single access point (AP), while LiFi system is assumed to follow different deployment schemes [83]: point Poisson process (PPP), Matern hard core point process (HCPP), regular square topology, and regular hexagonal topology (HEX). A single LiFi transmitter is composed by 18 individual transmitters (LEDs) arranged on a

semishpere. The semispheres, which act as access points, are assumed to be placed on the ceiling of the room. The distribution of the APs on the ceiling of the room follows the deployment schemes mentioned above.

Three different radii of HCPP deployment are assumed: 1 m, 1.7 m and 2.4 m. Legitimate users and eavesdroppers are assumed to be distributed as 2-D homogeneous PPPs in the room. As it can be seen in Fig. 12, LiFi transmitter with HEX deployment with 18-element transmitters can achieve over 8 times secrecy throughput improvement compared to WiFi. The 18 LED elements generates narrower light beams which can strongly reduce the SINR of eavesdroppers.

IV. CONCLUSION AND FUTURE DIRECTIONS

This paper envisioned the use of physical-layer security in future 6G networks. The unique characteristics of PLS can help in facing the significant security challenges raised by ubiquitous ultra-dense heterogeneous networks. The security features as well as practical implementations of PLS for 6G networks are discussed. Massive MIMO, IRS, LiFi or distributed and cooperative protocols are seen as possible PLS techniques to meet the 6G security requirements.

Open problems are still present: from the complete integration of PLS and higher-layers security protocols to the integration with AI, which is one of the main driver of 6G. The pervasive use of AI will surely provide benefits from security point of view, it also opens additional challenges since new threats could be opened, not known nowadays. PLS is envisioned to address the security threats coming from future 6G network. By applying AI technology, the PLS paradigm can be further improved compared with conventional security technologies.

In 5G the security-by-design approach has started to be considered, but the same treatment has not been given to the privacy. In a 360° security approach, as 6G is foreseen to provide, not only security-by-design has to be considered, but also privacy-by-design should be addressed.

REFERENCES

[1] M. Latva-Aho and K. Leppänen, "Key drivers and research challenges for 6G ubiquitous wireless intelligence," Oulu, Finland, 6G Res. Vis., Univ. Oulu, White Paper, 2019.

[2] R. A. Stoica and G. T. F. de Abreu, "6G: The wireless communications network for collaborative and AI applications," 2019. [Online]. Available: arXiv:1904.03413.

[3] P. Botsinis *et al.*, "Quantum algorithms for wireless communications," *IEEE Commmun. Surveys Tuts.*, vol. 21, no. 2, pp. 1209–1242, 2nd Quart., 2018.

[4] I. Ahmad, S. Shahabuddin, T. Kumar, J. Okwuibe, A. Gurtov, and M. Ylianttila, "Security for 5G and beyond," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 4, 3682–3722, 4th Quart., 2019.

[5] T. Pecorella, L. Brilli, and L. Mucchi, "The role of physical layer security in IoT: A novel perspective," *MDPI Inf.*, vol. 7, no. 3, pp. 49–66, 2016.

[6] S. Severi, G. T. F de Abreu, P. Gianni, and D. Dardari, "A secret key exchange scheme for near field communication," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, 2014, pp. 428–433.

[7] A. Francillon, B. Danev, and S. Čapkun, *Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars*, IACR, Lyon, France, 2011. [Online]. Available: https://eprint.iacr.org/2010/332.pdf

[8] 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.

[9] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1550–1573, 3rd Quart. 2014.

[10] 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.

[11] K. Zeng, K. Govindan, and P. Mohapatra, "Non-cryptographic authentication and identification in wireless networks," *IEEE Wireless Commun.*, vol. 17, no. 5, pp. 56–62, Oct. 2010.

[12] X. Duan and X. Wang, "Authentication handover and privacy protection in 5G HetNets using software-defined networking," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 28–35, Apr. 2015.

[13] Q. Xu, R. Zheng, W. Saad, and Z. Han, "Device fingerprinting in wireless networks: Challenges and opportunities," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 1, pp. 94–104, 1st Quart., 2016.

[14] M. Husák, J. Komárková, E. Bou-harb, and P. Čeleda, "Survey of attack projection, prediction, and forecasting in cyber security," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1, pp. 640–660, 1st Quart., 2019.

[15] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1773–1828, 2nd Quart., 2019.

[16] 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.

[17] A. Hyadi, Z. Rezki, and M. Alouini, "An overview of physical layer security in wireless communication systems with CSIT uncertainty," *IEEE Access*, vol. 4, pp. 6121–6132, 2016.

[18] L. Sun and Q. Du, "A review of physical layer security techniques for Internet of Things: Challenges and solutions," *Entropy*, vol. 20, no. 10, p. 730, Sep. 2018.

[19] D. Kapetanovic, G. Zheng, and F. Rusek, "Physical layer security for massive MIMO: An overview on passive eavesdropping and active attacks," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 21–27, Jun. 2015.

[20] W. K. Harrison, J. Almeida, M. R. Bloch, S. W. McLaughlin, and J. Barros, "Coding for secrecy: An overview of error-control coding techniques for physical-layer security," *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 41–50, Sep. 2013.

[21] W. Wang, K. C. Teh, K. H. Li, and S. Luo, "On the impact of adaptive eavesdroppers in multi-antenna cellular networks," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 2, pp. 269–279, Feb. 2018.

[22] K.-W. Huang, H.-M. Wang, Y. Wu, and R. Schober, "Pilot spoofing attack by multiple eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 17, no. 10, pp. 6433–6447, Oct. 2018.

[23] X. Zhou, B. Maham, and A. Hjorungnes, "Pilot contamination for active eavesdropping," *IEEE Trans. Wireless Commun.*, vol. 11, no. 3, pp. 903–907, Mar. 2012.

[24] Y. Wu, R. Schober, D. W. K. Ng, C. Xiao, and G. Caire, "Secure massive MIMO transmission with an active eavesdropper," *IEEE Trans. Inf. Theory*, vol. 62, no. 7, pp. 3880–3900, Jul. 2016.

[25] W. Wang, N. Cheng, K. C. Teh, X. Lin, W. Zhuang, and X. Shen, "On countermeasures of pilot spoofing attack in massive MIMO systems: A double channel training based approach," *IEEE Trans. Veh. Technol.*, vol. 68, no. 7, pp. 6697–6708, Jul. 2019.

[26] Q. Xiong, Y.-C. Liang, K. H. Li, and Y. Gong, "An energy-ratio-based approach for detecting pilot spoofing attack in multiple-antenna systems," *IEEE Trans. Inf. Forensics Security*, vol. 10, pp. 932–940, 2015.

[27] Y. Liu, H.-H. Chen, and L. Wang, "Physical layer security for next generation wireless networks: Theories, technologies, and challenges," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 347–376, 1st Quart., 2017.

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

[29] S. Mathur *et al.*, "Exploiting the physical layer for enhanced security [security and privacy in emerging wireless networks]," *IEEE Wireless Commun.*, vol. 17, no. 5, pp. 63–70, Oct. 2010.

[30] W. Trappe, R. Howard, and R. S. Moore, "Low-energy security: Limits and opportunities in the Internet of Things," *IEEE Security Privacy*, vol. 13, no. 1, pp. 14–21, Jan./Feb. 2015.

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

[32] R. Bassily *et al.*, "Cooperative security at the physical layer: A summary of recent advances," *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 16–28, Sep. 2013.

[33] G. Chisci, A. Conti, L. Mucchi, and M. Z. Win, "Intrinsic secrecy in inhomogeneous stochastic networks," *IEEE/ACM Trans. Netw.*, vol. 27, no. 4, pp. 1291–1304, Aug. 2019.

[34] 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.

[35] E. Del Re, S. Morosi, L. Mucchi, L. Ronga, and S. Jayousi, "Future wireless systems for human bond communications," *Wireless Pers. Commun.*, vol. 88, no. 1, pp. 39–52, May 2016.

[36] L. Mucchi, A. Martinelli, S. Jayousi, S. Caputo, and M. Pierobon, "Secrecy capacity and secure distance for diffusion-based molecular communication systems," *IEEE Access*, vol. 7, pp. 110687–110697, 2019.

[37] S. Xiao, W. Gong, and D. Towsley, "Secure wireless communication with dynamic secrets," in *Proc. IEEE INFOCOM*, San Diego, CA, USA, 2010, pp. 1–9.

[38] A. Garnaev, M. Baykal-Gursoy, and H. V. Poor, "A game theoretic analysis of secret and reliable communication with active and passive adversarial modes," *IEEE Trans. Wireless Commun.*, vol. 15, no. 3, pp. 2155–2163, Mar. 2016.

[39] S. Soderi, L. Mucchi, M. Hamalainen, A. Piva, and J. Iinatti, "Physical layer security based on spread-spectrum watermarking and jamming receiver," *Trans. Emerg. Telecommun. Technol.*, vol. 28, no. 7, pp. 1–13, Jul. 2017.

[40] L. Mucchi, L. Ronga, and L. Cipriani, "A new modulation for intrinsically secure radio channel in wireless systems,"*Wireless Pers. Commun.*, vol. 51, no. 1, pp. 67–80, Oct. 2009.

[41] M. Höyhtyä, O. Apilo, and M. Lasanen, "Review of latest advances in 3GPP standardization: D2D communication in 5G systems and its energy consumption models," *Future Internet*, vol. 10, no. 1, p. 3, Jan. 2018.

[42] T. L. Marzetta, "Noncooperative cellular wireless with unlimited numbers of base station antennas," *IEEE Trans. Wireless Commun.*, vol. 9, no. 11, pp. 3590–3600, Nov. 2010.

[43] E. Björnson, L. Sanguinetti, H. Wymeersch, J. Hoydis, and T. L. Marzetta, "Massive MIMO is a reality—What is next? Five promising research directions for antenna arrays," *Digit. Signal Process.*, vol. 94, pp. 3–20, Nov. 2019.

[44] S. Timilsina, D. Kudathanthirige, and G. Amarasuriya, "Physical layer security in cell-free massive MIMO," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Abu Dhabi, United Arab Emirates, Dec. 2018, pp. 1–7.

[45] T. M. Hoang, H. Q. Ngo, T. Q. Duong, H. D. Tuan, and A. Marshall, "Cell-free massive MIMO networks: Optimal power control against active eavesdropping," *IEEE Trans. Commun.*, vol. 66, no. 10, pp. 4724–4737, Oct. 2018.

[46] X. Zhang, D. Guo, and K. An, "Secure communication in multigroup multicasting cell-free massive MIMO networks with active spoofing attack," *Electron. Lett.*, vol. 55, no. 2, pp. 96–98, 2018.

[47] X. Zhang, D. Guo, K. An, Z. Ding, and B. Zhang, "Secrecy analysis and active pilot spoofing attack detection for multigroup multicasting cell-free massive MIMO systems," *IEEE Access*, vol. 7, pp. 57332–57340, 2019.

[48] M. Alageli, A. Ikhlef, F. Alsifiany, M. A. Abdullah, G. Chen, and J. Chambers, "Optimal downlink transmission for cell-free SWIPT massive MIMO systems with active eavesdropping," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 1983–1998, 2019.

[49] C. Huang, A. Zappone, G. C. Alexandropoulos, M. Debbah, and C. Yuen, "Reconfigurable intelligent surfaces for energy efficiency in wireless communication," *IEEE Trans. Wireless Commun.*, vol. 18, no. 8, pp. 4157–4170, Aug. 2019.

[50] S. Hu, F. Rusek, and O. Edfors, "Beyond massive MIMO: The potential of data transmission with large intelligent surfaces," *IEEE Trans. Signal Process.*, vol. 66, no. 10, pp. 2746–2758, May 2018.

[51] *NTT DoCoMo and Metawave Announce Successful Demonstration of 28GHz-Band 5G Using World's First Meta-Structure Technology*. Accessed: Jul. 7, 2019. [Online]. Available: https://www.marketwatch.com/press-release/ntt-docomo-and-metawave-announce-successful-demonstration-of-28ghz-band-5g-using-worlds-first-meta-structure-technology-2018-12-04

[52] 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.

[53] X. Yu, D. Xu, and R. Schober, "Enabling secure wireless communications via intelligent reflecting surfaces," in *Proc. IEEE Global Commun. Conf.*, Dec. 2019, pp. 1–6.

[54] H. Shen, W. Xu, S. Gong, Z. He, and C. Zhao, "Secrecy rate maximization for intelligent reflecting surface assisted multi-antenna communications," *IEEE Commun. Lett.*, vol. 23, no. 9, pp. 1488–1492, Sep. 2019.

[55] 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.

[56] D. Xu, X. Yu, Y. Sun, D. W. K. Ng, and R. Schober, "Resource allocation for secure IRS-assisted multiuser MISO systems," in *Proc. IEEE Global Commun. Conf.*, Dec. 2019, pp. 1–6.

[57] S. Zhang, H. Zhang, B. Di, Y. Tan, Z. Han, and L. Song, "Beyond intelligent reflecting surfaces: Reflective-transmissive metasurface aided communications for full-dimensional coverage extension," *IEEE Trans. Veh. Technol.*, vol. 69, no. 11, pp. 13905–13909, Nov. 2020.

[58] H. Haas, L. Yin, Y. Wang, and C. Chen, "What is LiFi?" *J. Lightw. Technol.*, vol. 34, no. 6, pp. 1533–1544, Mar. 15, 2016.

[59] T. Cogalan, H. Haas, and E. Panayirci, "Optical spatial modulation design," *Philosoph. Trans. Royal Soc. A*, vol. 378, no. 2169, pp. 1–18, Feb. 2020.

[60] A. Yesilkaya, E. Basar, F. Miramirkhani, E. Panayirci, M. Uysal, and H. Haas, "Optical MIMO-OFDM with generalized LED index modulation," *IEEE Trans. Commun.*, vol. 65, no. 8, pp. 3429–3441, Aug. 2017.

[61] E. Panayirci, A. Yesilkaya, T. Cogalan, H. Haas, and H. V. Poor, "Physical-layer security with generalized space shift keying," *IEEE Trans. Commun.*, vol. 68, no. 5, pp. 3042–3056, May 2020.

[62] N. Su, E. Panayirci, M. Koca, A. Yesilkaya , H. V. Poor, and H. Haas, "Physical layer security for multi-user MIMO visible light communication systems with generalized space shift keying," *IEEE Trans. Commun.*, vol. 69, no. 4, pp. 2585–2598, Apr. 2021.

[63] S. R. Aghdam and T. M. Duman, "Physical layer security for space shift keying transmission with precoding," *IEEE Wireless Commun. Lett.*, vol. 5, no. 2, pp. 180–183, Apr. 2016.

[64] Y. Chen, L. Wang, Z. Zhao, M. Ma, and B. Jiao, "Secure multiuser MIMO downlink transmission via precoding-aided spatial modulation," *IEEE Commun. Lett.*, vol. 20, no. 6, pp. 1116–1119, Jun. 2016.

[65] F. Wu, R. Zhang, L.-L. Yang, and W. Wang, "Transmitter precoding-aided spatial modulation for secrecy communications," *IEEE Trans. Veh. Technol.*, vol. 65, no. 1, pp. 467–471, Jan. 2016.

[66] A. Arafa, E. Panayirci, and V. H. Poor, "Relay-aided secure broadcasting for visible light communications," *IEEE Trans. Commun.*, vol. 67, no. 6, pp. 4227–4239, Jun. 2019.

[67] Z. Huang, Z. Gao, and L. Sun, "Anti-eavesdropping scheme based on quadrature spatial modulation," *IEEE Commun. Lett.*, vol. 21, no. 3, pp. 532–535, Mar. 2017.

[68] F. Wang, R. Li, J. Zhang, S. Shi, and C. Liu, "Enhancing the secrecy performance of the spatial modulation aided VLC systems with optical jamming," *Signal Process.*, vol. 157, pp. 288–302, Apr. 2019.

[69] L. Yin and H. Haas, "Physical-layer security in multiuser visible light communication networks," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 1, pp. 162–174, Jan. 2018.

[70] Y. Yang and M. Guizani, "Mapping-varied spatial modulation for physical layer security: Transmission strategy and secrecy rate," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 877–889, Apr. 2018.

[71] X. Jiang, M. Wen, H. Hai, J. Li, and S. Kim, "Secrecy-enhancing scheme for spatial modulation," *IEEE Commun. Lett.*, vol. 22, no. 3, pp. 550–553, Mar. 2018.
[72] N. Valliappan, A. Lozano, and R. W. Heath, "Antenna subset modulation for secure millimeter-wave wireless communication," *IEEE Trans. Commun.*, vol. 61, no. 8, pp. 3231–3245, Aug. 2013.
[73] F. Wang *et al.*, "Secrecy analysis of generalized space-shift keying aided visible light communication," *IEEE Access*, vol. 6, pp. 18310–18324, 2018.
[74] J. Wang, H. Ge, M. Lin, J. Wang, J. Dai, and M. Alouini, "On the secrecy rate of spatial modulation-based indoor visible light communications," *IEEE J. Sel. Areas Commun.*, vol. 37, no. 9, pp. 2087–2101, Sep. 2019.
[75] F. Shu, Z. Wang, R. Chen, Y. Wu, and J. Wang, "Two high-performance schemes of transmit antenna selection for secure spatial modulation,"*IEEE Trans. Veh. Technol.*, vol. 67, no. 9, pp. 8969–8973, Sep. 2018.
[76] A. A. Purwita, M. D. Soltani, M. Safari, and H. Haas, "Handover probability of hybrid LiFi/RF-based networks with randomly-oriented devices," in *Proc. IEEE 87th Veh. Technol. Conf. (VTC Spring)*, Porto, Portugal, Jun. 2018, pp. 1–5.
[77] E. Panayirci, "Optical index-coded space shift keying (IC/SSK)," *IEEE Commun. Lett.*, early access, May 25, 2021, doi: 10.1109/LCOMM.2021.3082866.
[78] N. Su, E. Panayirci, H. V. Poor, and M. Koca, "Spatial constellation design based generalized space shift keying for physical layer security of multi-user MIMO communication system," *IEEE Wireless Commun. Lett.*, vol. 10, no. 8, pp. 1785–1789, Aug. 2021, doi: 10.1109/LWC.2021.3079875.
[79] G. Pan, J. Ye, and Z. Ding, "Secure hybrid VLC-RF systems with light energy harvesting," *IEEE Trans. Commun.*, vol. 65, no. 10, pp. 4348–4359, Oct. 2017.
[80] L. Li, Y. Zhang, B. Fan, and H. Tian, "Mobility-aware load balancing scheme in hybrid VLC-LTE networks," *IEEE Commun. Lett.*, vol. 20, no. 11, pp. 2276–2279, Nov. 2016.
[81] M. Kashef, M. Abdallah, and N. Al-Dhahir, "Transmit power optimization for a hybrid PLC/VLC/RF communication system," *IEEE Trans. Green Commun. Netw.*, vol. 2, no. 1, pp. 234–245, Mar. 2018.
[82] J. Al-khori, G. Nauryzbayev, M. Abdallah, and M. Hamdi, "Physical layer security for hybrid RF/VLC DF relaying systems," in *Proc. IEEE 88th Veh. Technol. Conf. (VTC-Fall)*, Aug. 2018, pp. 1–6.
[83] M. A. Arfaoui *et al.*, "Physical layer security for visible light communication systems: A survey," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 3, pp. 1887–1908, 3rd Quart., 2020.
[84] Z. Chen and H. Haas, "Physical layer security for optical attocell networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, 2017, pp. 1–6.