IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received April 26, 2020, accepted May 13, 2020, date of publication May 21, 2020, date of current version June 10, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2996383

Safeguarding MTC at the Physical Layer: Potentials and Challenges

DIANA PAMELA MOYA OSORIO[1], (Member, IEEE), EDGAR EDUARDO BENITEZ OLIVO[2], (Member, IEEE), HIRLEY ALVES[1], (Member, IEEE), AND MATTI LATVA-AHO[1], (Senior Member, IEEE)

[1]Centre for Wireless Communications, University of Oulu, 90014 Oulu, Finland
[2]São Paulo State University (UNESP), Campus of São João da Boa Vista, São João da Boa Vista 13876-750, Brazil

Corresponding author: Diana Pamela Moya Osorio (diana.moyaosorio@oulu.fi)

This work was supported in part by the Academy of Finland 6Genesis Flagship under Grant 318927, in part by the European Union's Horizon 2020 Research and Innovation Program through the INSPIRE-5Gplus Project under Grant 871808, in part by the EE-IoT Project under Grant 319008, and in part by the Brazilian National Council for Scientific and Technological Development (CNPq) under Grant 421850/2018-3.

ABSTRACT 5G networks must provide a highly resilient, secure, and privacy-protected platform to support the emergence of new business and technologies expected from the so-called vertical-industry paradigm. However, as the definition and implementation of 5G networks are in progress, many security challenges arise. Thus, special emphasis will be given in the coming years to provide security and privacy for 5G and beyond networks. In this regard, physical layer security has been recognized as a potential solution to safeguard the confidentiality and privacy of communications in such stringent scenarios. In light of this, herein we provide an overview on some promising physical-layer techniques, focusing on the requirements and design challenges for machine-type communication scenarios. Key issues are discussed along with potential solutions.

INDEX TERMS Critical and massive Machine-Type Communications (mMTCs), Internet of Things (IoT), Physical layer security, 5G and beyond networks.

I. INTRODUCTION

5G and beyond networks are envisioned to support a wide range of use cases for a myriad of industry sectors. For that reason, the International Telecommunication Union (ITU) has classified 5G network services into three categories: enhanced Mobile Broadband (eMBB), Ultra-Reliable and Low-Latency Communication (URLLC), and massive Machine-Type Communication (mMTC). These services are suppose to coexist in the same network architecture by allocating network resources in such a way that the isolation among different inner logical networks (slices) is ensured through network slicing [1]. Particularly, in MTC networks, devices can be connected to the Internet or directly to each other, so that communication processes occur with little or no human intervention. This way, MTC plays a pivotal role on the concretization of the Internet of Things (IoT) and Internet of Everything (IoE) [2], [3]. Therefore, it can be said that, according to the service, MTC applications can be divided into two main groups: mMTC and critical (cMTC) [3].

mMTC comprehends scenarios with a large number of low-complexity and low-power devices, such as sensors and actuators, which are connected to a base station, using short-range radios and short-overhead protocols (as in capillary networks [4]) in order to allow for battery life savings. Then, mMTC focuses on high-density applications, such as smart wearables, smart agriculture, sensor networks, and smart meters. On the other hand, cMTC refers to applications with stringent requirements on availability, low latency, and reliability, such as traffic safety/control, remote surgery, vehicle-to-everything (V2X) networks, tactile Internet, and industrial control. For the case of cMTC, cost and energy constraints are not as critical as for mMTC applications.

Considering such heterogeneous requirements, it can be glimpsed that communication security is one of the main concerns for the deployment of MTC networks, since highly sensitive information will be transmitted over unprotected environments, thus being highly vulnerable to a plethora of security and privacy threats. This way, the design of secure MTC networks is a very challenging task that will demand

The associate editor coordinating the review of this manuscript and approving it for publication was Jason R. C. Nurse.

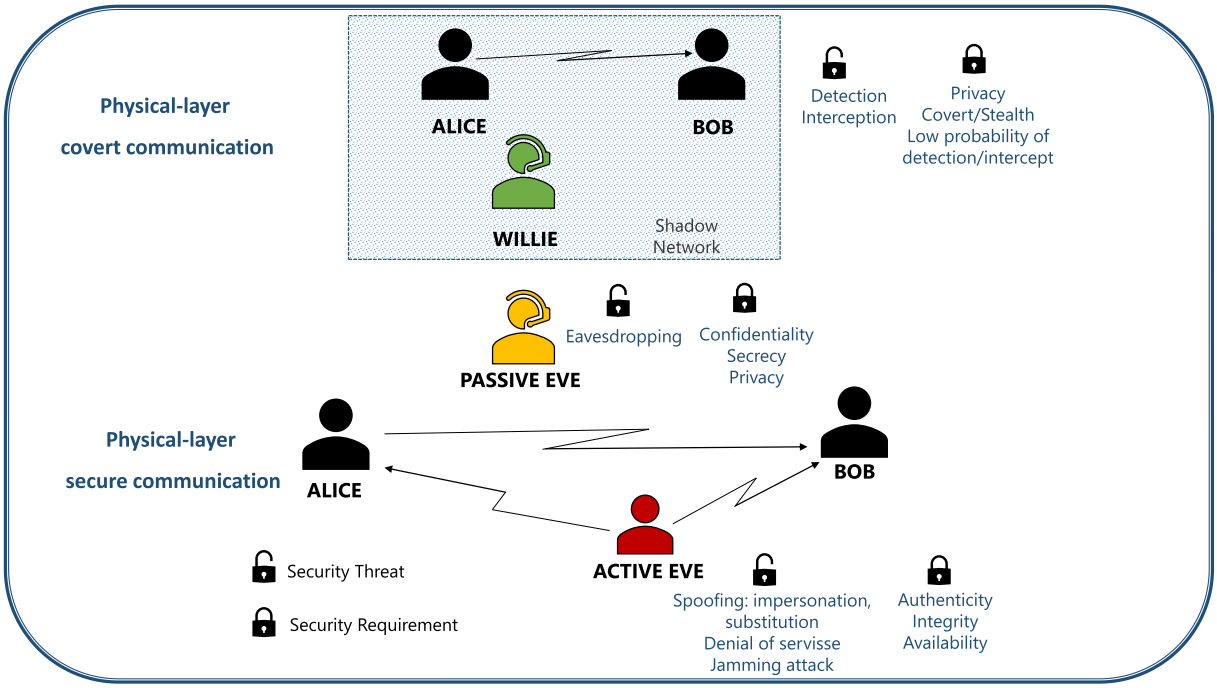

FIGURE 1. Security threats and requirements for secure and covert wireless communications.

lightweight and efficient solutions that attends the restrictions and the different requirements of mMTC and cMTC applications. Considering this, it has been recognized that traditional cryptography-based techniques, which are carried out at upper layers of data communication models, are not suitable to comply with the requirements of many MTC scenarios due to the following drawbacks: (*i*) the management of public-key cryptographic methods is extremely challenging in large-scale and decentralized networks as devices may randomly connect to or leave the network (or alternate between active and inactive states) at any moment [5]; (*ii*) secure links required for the exchange of private keys cannot be guaranteed in some MTC scenarios; (*iii*) eavesdropping and active attacks are facilitated by the rapid evolution of computing and processing capabilities, specially considering quantum computers; and (*iv*) demands for extra delay and complexity to provide strong security are undesirable for the MTC requirements.

Under these considerations, physical-layer (PHY) security has shown to be an attractive solution to avoid the heavy dependence on complicated traditional cryptography, thus being a promising technique to complement existing security techniques [6]. There are many reasons why PHY security has raised such an attention. For instance, it can be implemented in convenient ways without overburdening the resources or infrastructure of the network [7], [8]. Importantly, PHY security has the potential to be performed faster than other upper layer techniques.

PHY security relies on exploiting the physical properties and randomness of wireless channels, thus being particularly appealing in resource-limited application scenarios. Over the last years, a copious number of schemes and techniques have been proposed and analyzed, enriching the understanding on the potentials of this technology. Among the most important enabling approaches on PHY security we can mention the following: secrecy-achieving channel coding, diversity-aided secrecy techniques (such as multiple-input multiple-output (MIMO) and relaying systems), injection of artificial noise (friendly jamming), physical layer authentication (PLA), and physical layer key generation. We encourage the readers to find interesting detailed information on those and other techniques in [7], [8]. On the other hand, very recently, techniques related to physical-layer covert communications have gained attention in the context of security for 5G and beyond networks, since those techniques can prevent a legitimate transmission from being detected by an adversary, thus diminishing the possibility of eavesdropping attacks even if the adversary possesses unlimited processing resources (as in the case of quantum attacks). Thus, those techniques can guarantee a high level of security for MTC in very stringent scenarios [9], [10].

Despite the significant advances achieved so far regarding PHY security, as one of the most promising techniques to help attain the security level required for the scenarios of 5G and beyond networks, many challenging issues remain open for further research. In Fig. 1, we illustratively summarize some threats and requirements to be satisfied in the context of secure and covert communications.

A. CHARACTERISTICS OF MACHINE-TYPE COMMUNICATIONS

Herein, we introduce the main characteristics of both categories of MTC applications, namely, mMTC and cMTC, which will guide the discussions in the following sections.

For the mMTC category, the main objective is to connect a high density of low-rate, low-power, and low-complexity devices—the so-called Machine-Type Devices (MTDs)—to the cellular network (around 10^5 to 10^6 devices/km^2) [2]. These connections are uplink dominant, asynchronous, and sporadic, in which small data payloads are transmitted. In this sense, a random subset of devices are active at a given transmission instant, and the activation pattern can be periodic or event based. Additionally, MTDs are often battery powered, such that there exist a requirement of more than 10 years of autonomy [2]. Therefore, access and communication schemes should be highly energy efficient.

For the cMTC category, the main requirements are ultra-low latency and extremely high reliability performance [11]. The target packet loss probability is on the scale of 10^{-5} to 10^{-9}. For cMTC, it is also expected to have ultra availability up to 99.9999% with low to medium data rates (50 kbps to 10 Mbps) as in most cases the messages are small. Moreover, in terms of latency, the target is 1 ms Round-Trip Time (RTT) over-the-air communication for a single transmission, including the transmission of the payload until the corresponding acknowledgment is received [11].

Considering the above description of MTC use cases, in the following sections we highlight some of the most prominent aspects to be addressed for safeguarding future MTC networks at the PHY layer, for which an overview and some challenging points are provided.

II. EFFECTIVE DESIGN OF FINITE BLOCKLENGTH WIRETAP CODES

Traditionally, wiretap codes, mostly based on polar, lattice, or low-density-parity-check (LDPC) codes, are evaluated and analyzed as the blocklength approaches infinity, using information-theoretic security measures, where error probability and information leakage can asymptotically be extinguished, such that the maximum achievable secrecy rate is given by the secrecy capacity defined in [12]. Nonetheless, for some MTC scenarios, short blocklengths are more appropriated. Particularly, mMTC deployments of IoT will mostly consider energy-constrained devices that transmit only short packets. Also, the use of short packets is mandatory for minimizing the communication latency, which is imperative for delay-constrained scenarios in cMTC networks. In this context, while most popular coding schemes such as LDPC, Turbo codes and Polar codes have similar performance with large blocklengths, this is not the rule with short blocklengths, where significant differences can be noticed [13]. For finite blocklength wiretap codes, a tradeoff among error probability, information leakage, and transmission rate is established [14]. Thus, the knowledge of the complexity and performance of different wiretap code designs and their optimization at the finite blocklength is imperative for an effective application on practical MTC scenarios. Recently, best binary wiretap codes properties at the finite blocklength were analyzed in [15], [16], where it was shown that the equivocation ensured by coset coding over a binary erasure wiretap channel can be calculated with the knowledge of the full-rank submatrices of the generator matrix, which results in computational savings when optimizing wiretap codes at finite blocklength.

Also very recently, a flexible design for the wiretap code encoder and decoder in Gaussian wiretap channels under finite blocklength, based on a feed-forward neural network was proposed in [17], wherein a higher flexibility in terms of the error rate and leakage tradeoff was attained when compared to traditional error correcting codes.

Even though these promising solutions open the door for the future employment of PHY security techniques into practical MTC applications, there is still some challenges ahead in order to identify the best suited channel coding schemes. This way, for critical scenarios, bit-level granularity of the codeword size and flexibility to enable hybrid automatic repeat request (HARQ) are highly desired characteristics [13]. Moreover, techniques to identify best coding structures can be extremely helpful. For instance, in [18] was proposed a technique for analysing and comparing wiretap codes at the short blocklength regime over the binary erasure wiretap channel. In that work, the authors proposed Monte Carlo strategies for quantifying code's equivocation by limiting the analysis to coset-based wiretap codes. After several comparisons of different code families, the authors shown that using algebraic codes is advantageous for applications that require small-to-medium blocklengths.

Therefore, the design of practical wiretap codes that not only achieve the secrecy capacity limit at the finite blocklength regime, but also satisfy the constrains of MTC scenarios and heterogeneous environments (including highly dynamic or poor scattering environments where a strong correlation between legitimate and wiretap channels can occur [8]) remains a challenging task.

III. IMPACT OF CHANNEL STATE INFORMATION

Several PHY security approaches, specially those related to friendly jamming and diversity-aided security strongly rely on idealized assumptions, such as the perfect knowledge of the channel state information (CSI). This strong assumption imposes big challenges for the use of most wireless PHY security schemes in MTC applications, since an accurate estimation of CSI is a difficult task in practice, for both amplitude and phase information.

In most practical scenarios, the channel gains are measured by the receiver and then fed back to the transmitter. Such process can introduce imprecision and delays into the CSI, thus affecting the performance of PHY security techniques. At least, a certain level of CSI knowledge is required at the transmitter to attain a positive secrecy rate for a secure transmission. That is, the statistics of the channels should be known at the transmitter [19]. However, in some cases, where an eavesdropper remains passive, the statistics of the wiretap channel cannot be obtained at the transmitter. It is of interest to dedicate effort on solutions that do not rely on CSI knowledge—specially on that of the wiretap channel— thus

being suitable for delay-constrained applications as those of cMTC networks.

Moreover, the acquisition of CSI for MTC-based applications will bring a huge feedback overhead, specifically in massive deployments of IoT [20]. However, the data traffic pattern generated by MTC devices is typically sporadic. Then, by exploiting the sparsity in the device activity pattern, it can be possible to explore more efficient schemes to support simultaneous device activity detection and channel estimation [20]. This characteristic of some MTC deployments can be exploited to introduce security into communications at the physical layer. For instance, the sparsity in the MTC devices activity pattern can optimally be exploited by compressing sensing (CS) techniques in order to detect the active devices and estimate the channel conditions [20]. At the same time, some works have pointed out the ability of CS to ensure security [21], [22]. Indeed, by using CS, the channel asymmetry can be exploited in order to allow a message, encoded as a sparse vector, to be decodable with high probability at the legitimate receiver while being unfeasible to be decoded with high probability at the eavesdropper [21]. Particularly, in [22], the authors proposed a CS security model for IoT applications by exploiting the circulant matrix to improve the generating efficiency of the measurement matrix, while using a binary resilient function to guarantee security. Also, in [23], it was shown that physical layer security of a multi-hop relay network can be achieved by CS, without channel state information of the eavesdropper. Besides, individual sparsity patterns of devices can be predicted and used as fingerprints to perform fast physical layer authentication [24].

In light of these advances, exploring less complex secure CS techniques as well as improved techniques for device activity detection and prediction constitute open research areas.

Additionally, the accurate CSI estimation is more critical when considering multiple antennas. Indeed, in some MTC scenarios, massive MIMO techniques might be applied in order to serve several users simultaneously, so that great benefits in terms of security against passive and active attacks can be attained. However, the pilot training period for CSI estimation is vulnerable to attackers that can contaminate the uplink pilot sequences by generating identical pilots in order to modify the estimation. This is referred to as a pilot contamination attack (PCA), which is critical in MIMO systems as the eavesdropper can obtain a better signal-to-noise ratio (SNR) after beamforming. For instance, in [25] the achievable secrecy rate for a massive MIMO system under active and passive eavesdroppers was derived, and a power-ratio-based active pilot attack detection scheme was investigated. Therein, it was shown that the information leakage rate vanishes asymptotically as the number of base station antennas grows. However, active pilot attacks cannot be asymptotically mitigated, thus the achievable secrecy rate vanishes by increasing the eavesdropper pilot power.

The standard method to reduce pilot contamination is known as regular pilot (RP), which consists on adjusting the length of pilot sequences while the transmission of pilot and data symbols is done separately within the coherence block in order to reduce interference in the channel estimation process. Other alternative is known as superimposed pilot (SP), which sends a superposition of pilot and data symbols, and allows the amount of samples that can be used for channel estimation and data transmission to be increased. In [26], RP and SP methods are compared in terms of the achievable rate for a multicell massive MIMO network. Therein, it was observed that SP is able to reduce pilot contamination at the expense of incorporating further coherent and non-coherent interference, thus limiting the system performance. Also, by optimizing the pilot length with RP, the average spectral efficiency and energy efficiency are comparable to SP when estimated pilot subtraction is used. Besides, when the pilot symbols are subtracted perfectly with SP, the spectral efficiency and energy efficiency are improved. Then, the authors suggest to use iterative decoding algorithms for further improvements of SP method.

Recently, PCA detection was investigated in the context of non-orthogonal multiple access (NOMA) in millimeter wave and massive MIMO 5G communication networks. NOMA systems are promissory for MTC networks once they can improve spectral efficiency and achieve massive connectivity with low transmission latency and signaling cost; however, having superposed signals imposes new challenges for securing those systems. In [27] a binary hypothesis test and a machine learning based detection framework were proposed to perform PCA detection for static and dynamic environments. The results of that work showed that the detection rate can approach 100% with 10^{-3} of false alarm rate in the static environment and above 95% in the dynamic environment.

In [28], a secure communication for time-division duplex multi-cell multi-user massive MIMO systems was investigated when an active eavesdropping performs PCAs. Therein, it was shown that decreasing the desired user's signal power can be beneficial to combat a strong active attack from an eavesdropper. Therefore, a data-aided secure downlink transmission scheme was proposed, which achieves significant secrecy rate gains compared with alternative approaches based on matched filter precoding with artificial noise generation and null space transmission. Moreover, the authors in [29] investigated the vulnerabilities of pilot sequence design methods in realistic massive MIMO networks, where the assumption of strict orthogonality between the pilot sequence set is relaxed. Thus, the pilot sequences set is non-orthogonal and every pilot sequence has a non-zero cross-correlation with other pilot sequences. However, the use of correlated pilots could make the massive MIMO network more susceptible to PCAs. To proof this point, the authors in [29] proposed an effective active attack strategy with correlated pilot sequences revealing that the user capacity region of the network is significantly reduced in the presence of the PCA, and the SINR requirements for the worst-affected users may not be satisfied even with an infinite number of antennas at the base station.

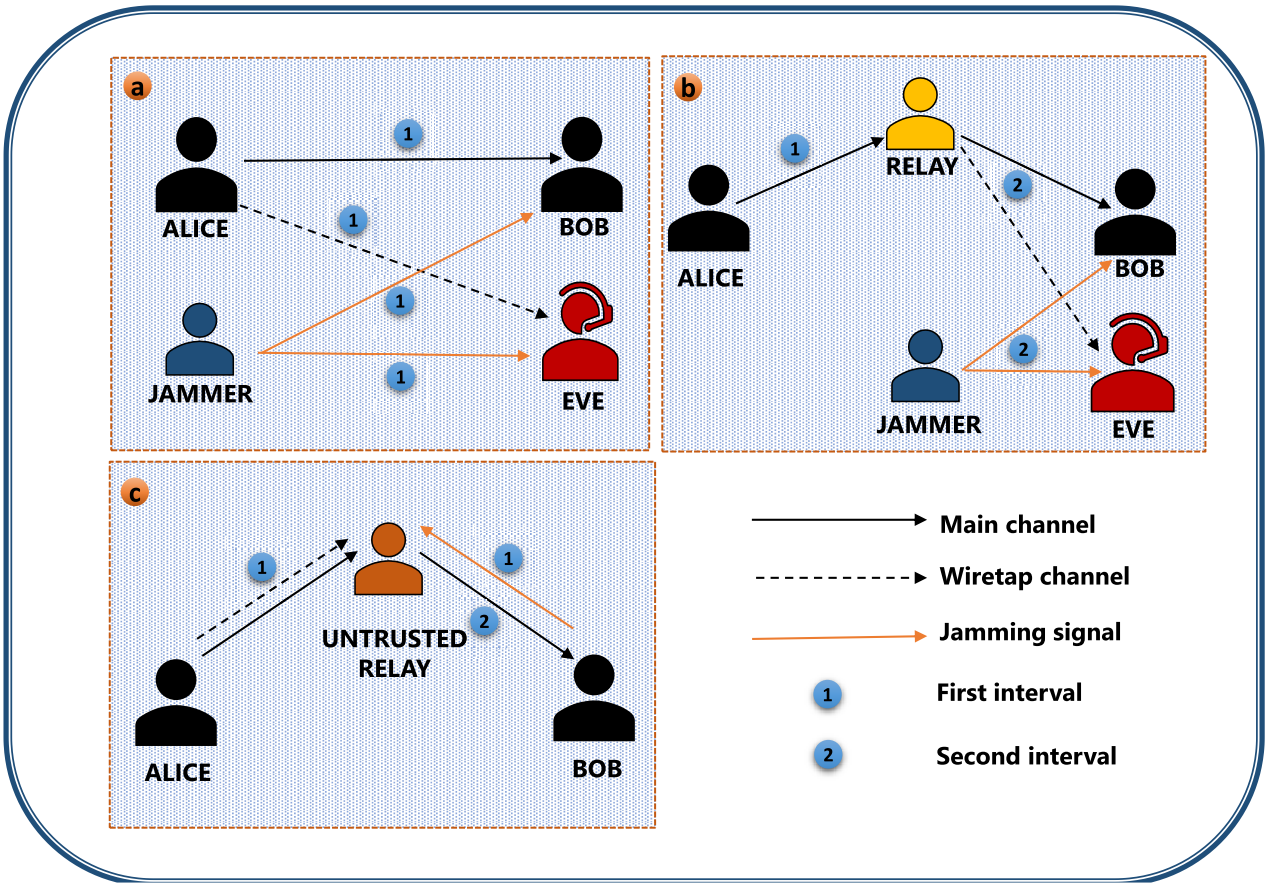

FIGURE 2. Different jamming strategies in physical layer security: a) cooperative jamming scenario with an external jammer, b) cooperative jamming scenario with a trusted relay and external jammer, and c) untrusted relay scenario with destination-based jamming.

IV. ROBUST JAMMING APPROACHES FOR PHYSICAL LAYER SECURITY

Friendly jamming strategies have proved to be promising as a way to degrade the channel quality of eavesdroppers for ensuring secret transmission by generating an artificial noise to confuse potential eavesdroppers. However, appropriate jamming strategies must be ensured in order to prevent the generation of undesired interference that can lead to a degradation on the performance of the legitimate channel or the information leakage to the eavesdroppers. Several strategies have already been proposed in the literature, including self and non-self cooperative jamming, jamming with perfect or imperfect eavesdropper's CSI, and uniform or directional jamming (some of them are illustrated in Fig. 2) [30].

In this sense, robust jamming strategies need to be designed in order to attain the benefits promised by those techniques. Particularly, the constraints on delay, energy, and massive deployments of MTC scenarios will give rise to special challenges for the utilization of jamming techniques in practical applications.

So far, game-theoretic approaches have emerged as attractive solutions to deal with the interactions among legitimate users, eavesdroppers and friendly jammers, which can be employed to make optimal decisions [31]. In game theory, agents are rational entities whose target is to maximize their individual gains or payoff functions. For instance, Stackelberg games have been used to model the interactions and power allocations between the legitimate pair and the friendly jammer as a seller-buyer interaction game, where the jammer is the seller and the legitimate pair are the buyers [32].

However, there is still a vast area to be explored in order to create more effective and suitable jamming strategies for the different constraints of different MTC applications. Therefore, the development of robust game-based jamming strategies that consider channel uncertainties or the lack of knowledge of eavesdroppers' CSI, in addition to energy and/or latency constraints, is an open challenge. For instance, Bayesian games have been suggested for scenarios with incomplete information where imperfect or no eavesdropper's CSI is available [31].

Additionally, the benefits of wireless energy transfer and energy harvesting technologies can be exploited to provide jamming strategies with an alternative source of energy for jammers, thus being more attractive for real-world IoT applications [33], [34].

V. IMPROVED PHYSICAL LAYER AUTHENTICATION AND SECRET-KEY GENERATION SCHEMES

Authentication methods target to verify the identity of the legitimate parts, thus preventing two types of spoofing

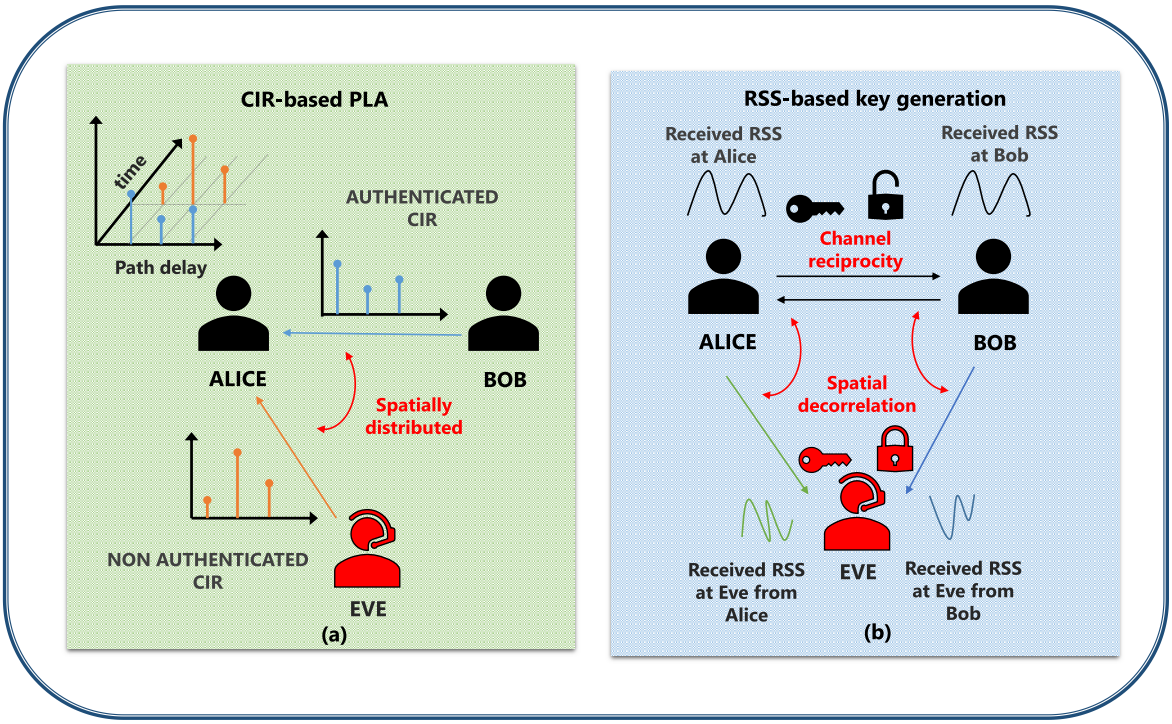

FIGURE 3. Schematics on (a) channel impulse response-based PHY authentication and (b) receive signal strength-based secret-key generation.

attacks, namely, impersonation and substitution. In the former, the attacker sends messages to a legitimate receiver in order to confuse it with other legitimate users, while in the latter, the attacker intercepts legitimate messages, modifies them and then retransmits the altered messages to legitimate users. These methods, traditionally conducted at upper layers, may result in exorbitant latencies in large-scale networks, whereas the limited resources of a massive number of heterogeneous devices from MTC applications will demand robust and lightweight authentication alternatives [35]. Moreover, because digital keys are generally used to identify and provide rights to users, attackers using unauthorized security keys cannot be efficiently detected in those scenarios, when physical-layer properties are overlooked. Therefore, physical-layer attributes of devices and environments, i.e., the so-called physical-layer device fingerprints, can be used to perform authentication with low computational power, energy and overhead requirements, while being robust as those attributes are hard to be mimicked or predicted. This technique is referred to as physical-layer authentication (PLA) [35]. Fingerprints can be of two types, channel-based fingerprints or analog front-end (AFE) imperfection-based fingerprints. Channel-based PLA exploits wireless channel parameters such as channel state information (CSI), received signal strength (RSS), channel frequency response (CFR), and channel impulse response (CIR), in order to design the authentication of devices, as depicted in Fig. 3(a). As a downside, this approach requires significant channel monitoring, which is subject to imperfect estimates, thus being critical in highly dynamic environments as those of V2X communications. On the other hand, the AFE imperfection-based PLA relies on specific characteristics introduced during the fabrication of devices, including in-phase and quadrature imbalance (IQI), digital-to-analog converter, carrier frequency offset, power amplifier, among others. In practice, the reliability of estimating differences among the aforementioned attributes can be deteriorated due to noise and dynamic interference conditions.

The authentication process must be carried out periodically during the secret message transmission, within the coherence time of the channel, in order to guarantee a sufficient agreement of the channel signatures. Therefore, due to the time-varying nature of these attributes and imperfect estimation, PLA techniques may be difficult to design and standardize, thus presenting low reliability and accuracy. However, multi-attribute authentication techniques can be used to improve the robustness and accuracy of PLA, by combining a number of selected attributes according to the specific application scenario, thus attaining an increased level of security in the presence of attackers [35]. On the other hand, the use of multiple attributes may lead to extremely complex searches in highly dynamic scenarios, whereas the adaptation of the PLA process requires to be performed almost instantaneously.

A. INCREASING THE ACCURACY AND ROBUSTNESS OF PLA

Machine learning (ML) as well as other artificial intelligence (AI) techniques can be used to improve the robustness of PLA, thus opening new opportunities for the

application of PLA techniques in practical MTC scenarios. For instance, in [36], a multi-attribute PLA was proposed, based on the kernel of a ML technique to avoid the requirement of knowing the statistical distribution of the attributes, such that a multi-dimensional space is reduced to a single dimension to decrease the authentication process complexity. Also, an adaptive algorithm was adopted for tracking the attribute variations in order to achieve a more reliable authentication performance.

B. IMPROVING EFFICIENCY DURING HANDOVERS IN HETEROGENEOUS NETWORKS

In future heterogeneous MTC networks, frequent handover and authentication processes, due to transfer of users between small cells, will inflict challenges in terms of latency, which is a crucial concern for cMTC. Therefore, improving the efficiency of the authentication process during a handover process is imperative for the deployment of future MTC networks. In this sense, the handover authentication process may not occur in a totally new context, so that many stable attributes can be predicted from their previous observations. For instance, physical-layer key generation, described next, has a huge potential to be used as a network-wide unique and unforgeable key, thus reducing some repetitive steps in cryptographic authentication schemes [35].

C. PHYSICAL-LAYER KEY GENERATION CHALLENGES

In physical layer key generation, wireless devices measure highly correlated wireless channel characteristics, such as CIR or RSS, and use those measurements as shared random sources to generate a shared key. The typical process followed by Alice and Bob to generate this secret key follows 5 steps as illustrated in Fig. 4 [37]. Regarding that process, physical-layer key generation is based on three principles, namely, temporal channel variation, channel reciprocity, and spatial decorrelation [37], [38] (as illustrated in Fig. 3(b)). Temporal channel variation is introduced by the movement of the transmitter, receiver, or surrounding objects in the environment. Channel reciprocity implies that bidirectional wireless channel states are identical between two transceivers during a given time interval, so that it is feasible to generate the same key. This is only valid for time division duplex (TDD) based systems. Spatial decorrelation indicates that the wireless channel properties are unique to the locations of the transceivers at the legitimate link, such that an eavesdropper at a position farther than one-half wavelength away from the legitimate transceivers experiences a different and uncorrelated channel state. However, these assumptions may not be satisfied in all the environments. Therefore, physical-layer key generation faces some challenges to be overcome before their efficient use in MTC networks.

For instance, in cases where the eavesdropper is co-located with Alice or Bob, it will observe channel measurements that are highly correlated, such that the communication is vulnerable to attacks. To prevent this issue, the authors in [39] proposed a solution for millimeter wave (mmWave) massive MIMO communication systems that relies on the high directionality of beams that can be attained by using massive-MIMO-based beamforming techniques.

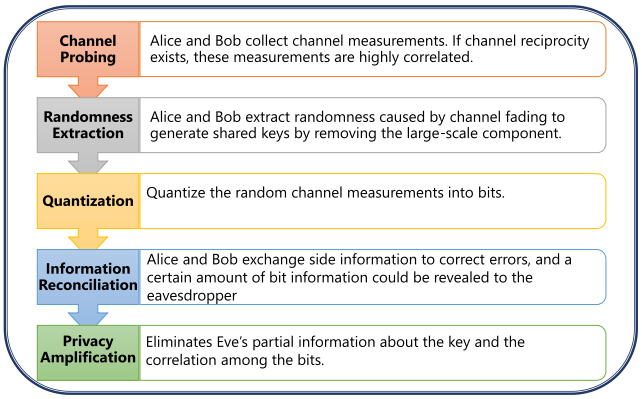

FIGURE 4. Typical physical layer key generation process.

Transceiver hardware, time delay in TDD systems as well as fine grain quantization may introduce disagreements in initial keys. Therefore, in the reconciliation step (forth step in Fig. 4), an error correction process with information exchange between Alice and Bob is carried out to improve the initial keys. Existing approaches include the cascade algorithm and LDPC codes. However, a significant reconciliation overhead can be introduced if the bit disagreement before the reconciliation is high [37], thus decreasing the key generation rate. To overcome this issue, the authors in [40] proposed two new channel characteristics, virtual AoA (Angle of Arrival) and AoD (Angle of Departure), in order to generate a shared secret key with low bit disagreement between two devices in mmWave Massive MIMO channel. This is attained by exploiting the sparsity and robusteness against noise of these channel characteristics.

Also, in wireless networks with multiple nodes—or with a massive number of nodes, as those of mMTC scenarios—group key generation schemes would be more appealing compared to one-by-one generation methods, especially for broadcast/multicast communications [41]. However, the key generation process may suffer from a high complexity, as more channels and more parameters for optimization need to be considered, thus requiring a longer channel coherence time, in addition to the risk of leaking information to eavesdroppers when sharing channel information to the various nodes.

Therefore, pursuing novel, robust and low-complex solutions for secret group-key generation schemes from physical layer characteristics is an appealing research area for providing security in MTC networks.

VI. INTEGRATION SECURITY IN THE RANDOM ACCESS

From the perspective of the uplink communication, providing scalable connectivity for a large number of devices with a sporadic and low data rate traffic pattern (such as in smart metering applications) is one of the primary challenges of

mMTC [2]. This contrasts with downlink-focused communications for human-centric services with high data rates, on which the design criteria for LTE and earlier cellular generations technologies relied on. In this context, non-orthogonal grant-free (rather than orthogonal grant-based) medium access control turns out to be more suitable for mMTC, as a certain degree of radio-resource overloading is allowed, at the cost of an augmented number of collisions and increased receiver complexity at the base station. Moreover, medium access protocols employed in current cellular networks demands a considerable signaling overhead, a large part of which is required to provide access, as well as authentication and security. Nonetheless, this is compensated since large-payload packets are employed, so that the protocol efficiency (defined as the ratio between the data and signaling overhead) is high. On the other hand, the protocol efficiency of traditional medium access protocols is compromised when considered the short-packet traffic pattern inherent to mMTC. Thus, new PHY and MAC layer technology solutions are needed to deal with a huge amount of asynchronous, low data-rate, small-packet, sporadic connections, so that the same functionality of existing access protocols in terms of radio resource reservation and security is achieved, but with significantly less signaling overhead. In this sense, mMTC traffic is shown to benefit significantly from signature-based random access schemes, which embed both authentication and security information, thus ensuring a high access reliability for increasing access loads, while reducing access latency and signaling overhead when compared to traditional access protocols [42]. Further solutions in this direction can be specially attractive for cMTC scenarios as well, which are characterized by stringent restrictions on high reliability and extremely low latency.

VII. PHYSICAL-LAYER COVERT COMMUNICATIONS

With the introduction of MTC, mMTC, and cMTC in 5G networks, we expect an exponentially increasing number of devices communicating with the most diverse requirements, not only in terms of data rate, reliability, and latency, but also in terms of security. Traditional cryptography techniques cannot cope with all security problems in MTC scenarios. For instance, if a MTC node intends to communicate covertly with another without being detected by an adversary, cryptography is not enough. An eavesdropper could infer information relative to a node, or even of the entire network, from the conveyed metadata (e.g., the network traffic pattern), which can reveal sensitive information about the users. Even though the eavesdropper is not able to decode the message, it could estimate the user's location or transmission behavior. Unlike traditional cryptography, covert wireless communications aims to hide the transmission behavior by providing covertness, stealth or low probability of detection for communications. Then, if a malicious entity cannot detect transmissions, there is no chance to perform an eavesdropping and decoding attack, even if unlimited resources or quantum potentialities are used.

In this context, PHY covert wireless communications have recently received increased attention from academia [9], [10]. In a PHY covert wireless communication system, privacy is preserved once the adversary is prevented from knowing the existence of transmissions by using PHY techniques or wireless channel properties, such as spread spectrum, friendly jammers, or background noise. For instance, the authors in [9] determined how much covert information can be transmitted reliably over additive white Gaussian noise (AWGN) channels. Therein, it was found a square root law according to which a legitimate source can transmit $\mathcal{O}(\sqrt{n})$ bits reliably and covertly to a legitimate destination over n channel uses, with the transmission power at the legitimate source being a decreasing function of the blocklength n.

More recently, by virtue of distinctive features of future MTC networks which are expected to be highly heterogeneous and dense, in [10] was proposed to leverage another kind of noise source (in addition to the background noise) in order to achieve covert communications, namely, the aggregated interference from other transmitters. In fact, the adversary's uncertainty on the aggregated interference is beneficial for the legitimate transmitter to remain covert, as the randomness of aggregated interference, which comes from random locations of potential transmitters and fading channels, is greater than the background noise. Furthermore, it was concluded in [10] that, from the network perspective, this approach of hiding communications in interference shows considerably higher spatial throughput, although the covert throughput for any pair of users may become lower.

In this instance, some challenges can be pointed out, as follows. It was demonstrated in [10] that hiding information in interference is effective when a static and passive eavesdropper is considered. This is appealing for mMTC scenarios where the eavesdropper will be overwhelmed by a dense wireless network with a large number of nodes, such that discriminating the actual transmitter from others in a network is a difficult task. However, if an active adversary is considered (i.e., an eavesdropper that dynamically adjust its distance to the legitimate transmitter, based on its observations), so that it can move to the vicinity of the legitimate transmitter, the strategy of hiding transmissions in interference could be compromised. This situation could be aggravated when considered multiple active adversaries, which can cooperate to improve their detection ability, or an adversary equipped with more antennas than the legitimate transmitter and receiver. In this sense, randomized transmission scheduling [43], cooperative jamming or coordinated interference mechanisms [44] can be explored as potential solutions to provide covert regions, where the private-message exchange can occur regardless of the computational power of the adversary, while providing location privacy preservation to the legitimate transceivers.

On the other hand, although the characteristics of MTC vary for different applications, it is a common assumption in the literature and for standardization bodies that MTC traffic will be dominated by small packages from periodic or asynchronous alarm-based transmissions. The square root

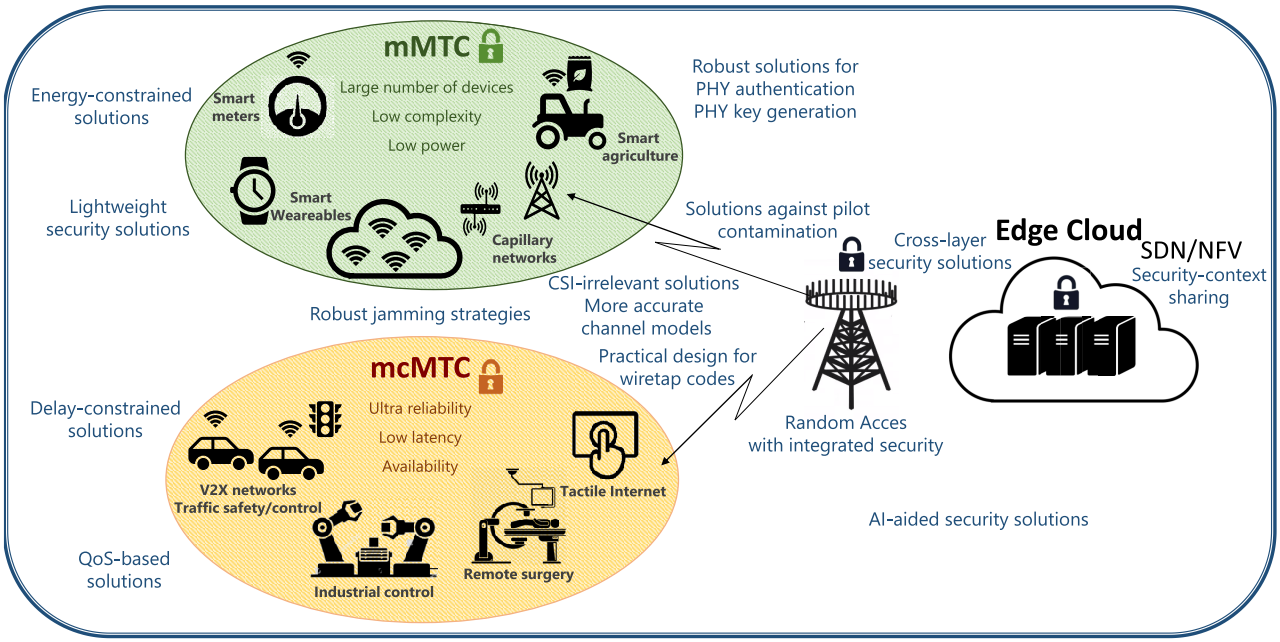

FIGURE 5. General view of physical layer security and key performance indicators for MTC networks.

law is attained with asymptotic assumptions on the number of channel uses; therefore, a better understanding of the fundamental limits of covert communications under practical limitations, where the codeword length is finite (in the order of hundreds of channel uses), is still an open issue.

VIII. CONCLUDING REMARKS

So far, we have provided a detailed overview on decisive aspects that need to be further investigated for securing MTC networks from the physical layer perspective, as well as some interesting solutions which are summarized in Fig. 5. In the following, we will discuss some key challenges relevant to those aspects.

A. PRACTICAL CHANNEL MODELS

Accurate channel models are crucial for the appropriate design of system parameters and system performance evaluation. In this sense, 5G networks bring huge challenges regarding the search for accurate channel models that efficiently fit 5G environments, as a wide diversity of scenarios need to be considered, such as indoor, urban, suburban, and rural areas, as well as rapid train and unmanned-aerial-vehicles (UAV) networks, among others. In addition, future approaches on PHY security techniques and metrics should be designed according to the challenges imposed by more practical and accurate channel models for MTC networks, which also consider extremely wide frequency bands (in the mm-Wave, THz, and visible light spectrum) and new scenarios (e.g., tunnel, underground, underwater, and even human body). A wide variety of scenario-specific 5G channel models have been already proposed in the literature (an excellent survey can be found in [45]). Then, it is essential to revise PHY security techniques and metrics regarding these new channel models [46]–[48]. Indeed, various PHY security techniques are invalidated in poor scattering environments where a strong correlation between legitimate and wiretap channels exists. Additionally, quasi-static and poor scattering channels can be challenging for secret key generation, whereas highly-dynamic channels are challenging for performing PLA. Moreover, physical-layer covert communications techniques are still limited to basic channel models, thus exploring its benefits in realistic scenarios is a big challenge ahead.

B. CROSS-LAYER TECHNIQUES

Performing different authentication processes at different protocol layers can increase the security level of MTC networks at the expense of increased complexity and latency, which should be avoided for the practical scenarios of MTC. Thus, cross-layer security approaches can be attractive to further improve the level of security and privacy in those scenarios, while reducing cost and overhead, by enabling the information exchange across different protocol layers or mixing the information from two or more layers in order to design security strategies that can comply with QoS, latency or energy constraints [3]. Then, these approaches deserve further attention, as exchanging information across layers can demand meticulous tasks to design efficient solutions.

C. MACHINE-LEARNING TECHNIQUES FOR PHY SECURITY

Very recently, a number of multi-attribute PLA approaches have been investigated by relying on the potentialities of ML techniques. These solutions have shown to be effective to

design robust and accurate PLA techniques, which will open great opportunities for the integration of PHY security in the design of 5G and beyond networks. However, regarding MTC networks, some important issues should be considered, as follows [49]: (*i*) the time consumed for the convergence of a given ML technique may reduce the time for data transmission, then this trade-off should be considered for the design, (*ii*) distributed implementation of the learning algorithm across multiple learning devices, (*iii*) parameters such as learning rate, discount rate, and exploration/exploitation trade-off should be dynamically adapted to enhance the performance of a Q-learning algorithm in highly dynamic environments, and (*iv*) the heterogeneity of MTC devices must be taken into account in terms of learning capability, cache size, delay tolerance, and data rate.

REFERENCES

[1] *Study on New Radio (NR) Access Technology Physical Layer Aspects*, 3GPP, document TR 38.802, Mar. 2017.

[2] C. Bockelmann, N. K. Pratas, G. Wunder, S. Saur, M. Navarro, D. Gregoratti, G. Vivier, E. De Carvalho, Y. Ji, Č. Stefanović, P. Popovski, Q. Wang, M. Schellmann, E. Kosmatos, P. Demestichas, M. Raceala-Motoc, P. Jung, S. Stanczak, and A. Dekorsy, "Towards massive connectivity support for scalable mMTC communications in 5G networks," *IEEE Access*, vol. 6, pp. 28969–28992, 2018.

[3] N. Huda Mahmood, H. Alves, O. Alcaraz López, M. Shehab, D. P. Moya Osorio, and M. Latva-aho, "Six key enablers for machine type communication in 6G," 2019, *arXiv:1903.05406*. [Online]. Available: http://arxiv.org/abs/1903.05406

[4] J. Sachs, N. Beijar, P. Elmdahl, J. Melen, F. Militano, and P. Salmela, "Capillary networks–a smart way to get things connected," *Ericsson Rev.*, vol. 91, pp. 1–8, Sep. 2014.

[5] 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.

[6] D. P. M. Osorio, J. D. V. Sanchez, and H. Alves, "Physical layer security for 5G and beyond," in *5G REF: The Essential 5G Reference Online*. Hoboken, NJ, USA: Wiley, 2020.

[7] 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.

[8] 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.

[9] B. A. Bash, D. Goeckel, and D. Towsley, "Limits of reliable communication with low probability of detection on AWGN channels," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1921–1930, Sep. 2013.

[10] Z. Liu, J. Liu, Y. Zeng, and J. Ma, "Covert wireless communications in IoT systems: Hiding information in interference," *IEEE Wireless Commun.*, vol. 25, no. 6, pp. 46–52, Dec. 2018.

[11] N. A. Mohammed, A. M. Mansoor, and R. B. Ahmad, "Mission-critical machine-type communication: An overview and perspectives towards 5G," *IEEE Access*, vol. 7, pp. 127198–127216, 2019.

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

[13] M. Shirvanimoghaddam, M. S. Mohammadi, R. Abbas, A. Minja, C. Yue, B. Matuz, G. Han, Z. Lin, W. Liu, Y. Li, S. Johnson, and B. Vucetic, "Short block-length codes for ultra-reliable low latency communications," *IEEE Commun. Mag.*, vol. 57, no. 2, pp. 130–137, Feb. 2019.

[14] W. Yang, R. F. Schaefer, and H. V. Poor, "Wiretap channels: Nonasymptotic fundamental limits," *IEEE Trans. Inf. Theory*, vol. 65, no. 7, pp. 4069–4093, Jul. 2019.

[15] W. K. Harrison and M. R. Bloch, "On dual relationships of secrecy codes," in *Proc. 56th Annu. Allerton Conf. Commun., Control, Comput. (Allerton)*, Oct. 2018, pp. 366–372.

[16] W. K. Harrison and M. R. Bloch, "Attributes of generators for best finite blocklength coset wiretap codes over erasure channels," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2019, pp. 827–831.

[17] K.-L. Besser, C. R. Janda, P.-H. Lin, and E. A. Jorswieck, "Flexible design of finite blocklength wiretap codes by autoencoders," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, May 2019, pp. 2512–2516.

[18] J. Pfister, M. A. C. Gomes, J. P. Vilela, and W. K. Harrison, "Quantifying equivocation for finite blocklength wiretap codes," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2017, pp. 1–6.

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

[20] T. Jiang, Y. Shi, J. Zhang, and K. B. Letaief, "Joint activity detection and channel estimation for IoT networks: Phase transition and computation-estimation tradeoff," *IEEE Internet Things J.*, vol. 6, no. 4, pp. 6212–6225, Aug. 2019.

[21] S. Agrawal and S. Vishwanath, "Secrecy using compressive sensing," in *Proc. IEEE Inf. Theory Workshop*, Oct. 2011, pp. 563–567.

[22] N. Wang, T. Jiang, W. Li, and S. Lv, "Physical-layer security in Internet of Things based on compressed sensing and frequency selection," *IET Commun.*, vol. 11, no. 9, pp. 1431–1437, Jun. 2017.

[23] L. Qing, H. Guangyao, and F. Xiaomei, "Physical layer security in multi-hop AF relay network based on compressed sensing," *IEEE Commun. Lett.*, vol. 22, no. 9, pp. 1882–1885, Sep. 2018.

[24] G. Wunder, H. Boche, T. Strohmer, and P. Jung, "Sparse signal processing concepts for efficient 5G system design," *IEEE Access*, vol. 3, pp. 195–208, 2015.

[25] R. F. Schaefer, G. Amarasuriya, and H. V. Poor, "Physical layer security in massive MIMO systems," in *Proc. 51st Asilomar Conf. Signals, Syst., Comput.*, Oct. 2017, pp. 3–8.

[26] D. Verenzuela, E. Bjornson, and L. Sanguinetti, "Spectral and energy efficiency of superimposed pilots in uplink massive MIMO," *IEEE Trans. Wireless Commun.*, vol. 17, no. 11, pp. 7099–7115, Nov. 2018.

[27] N. Wang, L. Jiao, A. Alipour-Fanid, M. Dabaghchian, and K. Zeng, "Pilot contamination attack detection for NOMA in 5G mm-wave massive MIMO networks," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 1363–1378, 2020.

[28] Y. Wu, C.-K. Wen, W. Chen, S. Jin, R. Schober, and G. Caire, "Data-aided secure massive MIMO transmission under the pilot contamination attack," *IEEE Trans. Commun.*, vol. 67, no. 7, pp. 4765–4781, Jul. 2019.

[29] N. Akbar, S. Yan, A. M. Khattak, and N. Yang, "On the pilot contamination attack in multi-cell multiuser massive MIMO networks," *IEEE Trans. Commun.*, vol. 68, no. 4, pp. 2264–2276, Apr. 2020, doi: 10.1109/TCOMM.2020.2967760.

[30] Y. Huo, Y. Tian, L. Ma, X. Cheng, and T. Jing, "Jamming strategies for physical layer security," *IEEE Wireless Commun.*, vol. 25, no. 1, pp. 148–153, Feb. 2018.

[31] K. Cumanan, H. Xing, P. Xu, G. Zheng, X. Dai, A. Nallanathan, Z. Ding, and G. K. Karagiannidis, "Physical layer security jamming: Theoretical limits and practical designs in wireless networks," *IEEE Access*, vol. 5, pp. 3603–3611, 2017.

[32] A. Wang, Y. Cai, W. Yang, and Z. Hou, "A stackelberg security game with cooperative jamming over a multiuser OFDMA network," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Apr. 2013, pp. 4169–4174.

[33] H. Xing, Z. Chu, Z. Ding, and A. Nallanathan, "Harvest-and-jam: Improving security for wireless energy harvesting cooperative networks," in *Proc. IEEE Global Commun. Conf.*, Dec. 2014, pp. 3145–3150.

[34] E. N. Egashira, E. E. Benitez Olivo, D. P. Moya Osorio, and H. Alves, "Secrecy performance of untrustworthy AF relay networks using cooperative jamming and SWIPT," in *Proc. IEEE 30th Annu. Int. Symp. Pers., Indoor Mobile Radio Commun. (PIMRC)*, Sep. 2019, pp. 1–6.

[35] 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.

[36] H. Fang, X. Wang, and L. Hanzo, "Learning-aided physical layer authentication as an intelligent process," *IEEE Trans. Commun.*, vol. 67, no. 3, pp. 2260–2273, Mar. 2019.

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

[38] 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.

[39] X. Ji, K. Huang, L. Jin, H. Tang, C. Liu, Z. Zhong, W. You, X. Xu, H. Zhao, J. Wu, and M. Yi, "Overview of 5G security technology," *Sci. China Inf. Sci.*, vol. 61, no. 8, Jul. 2018, Art. no. 081301.

[40] L. Jiao, J. Tang, and K. Zeng, "Physical layer key generation using virtual AoA and AoD of mmWave massive MIMO channel," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, May 2018, pp. 1–9.

[41] C. D. T. Thai, J. Lee, J. Prakash, and T. Q. S. Quek, "Secret group-key generation at physical layer for multi-antenna mesh topology," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 1, pp. 18–33, Jan. 2019.

[42] N. K. Pratas, S. Pattathil, C. Stefanovic, and P. Popovski, "Massive machine-type communication (mMTC) access with integrated authentication," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2017, pp. 1–6.

[43] Z. Liu, J. Liu, Y. Zeng, J. Ma, and Q. Huang, "Covert wireless communications with active eavesdropper on AWGN channels," 2018, *arXiv:1805.06182*. [Online]. Available: http://arxiv.org/abs/1805.06182

[44] R. Soltani, D. Goeckel, D. Towsley, B. A. Bash, and S. Guha, "Covert wireless communication with artificial noise generation," *IEEE Trans. Wireless Commun.*, vol. 17, no. 11, pp. 7252–7267, Nov. 2018.

[45] C.-X. Wang, J. Bian, J. Sun, W. Zhang, and M. Zhang, "A survey of 5G channel measurements and models," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 3142–3168, 4th Quart., 2018.

[46] P. Ramirez-Espinosa, R. J. Sanchez-Alarcon, and F. J. Lopez-Martinez, "On the beneficial role of a finite number of scatterers for wireless physical layer security," 2019, *arXiv:1910.09856*. [Online]. Available: https://arxiv.org/abs/1910.09856

[47] J. D. V. Sanchez, D. P. M. Osorio, E. E. B. Olivo, H. Alves, M. C. P. Paredes, and L. U. Aguiar, "On the statistics of the ratio of nonconstrained arbitrary $\alpha - \mu$ random variables: A general framework and applications," *Trans. Emerg. Telecommun. Technol.*, vol. 31, no. 3, p. e3832, 2020. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/ett.3832

[48] J. D. V. Sanchez, D. P. M. Osorio, F. J. Lopez-Martinez, M. C. Paredes, and L. Urquiza-Aguiar, "On the secrecy performance over N-wave with diffuse power fading channel," 2020, *arXiv:2002.05206*. [Online]. Available: https://arxiv.org/abs/2002.05206

[49] S. Krishna Sharma and X. Wang, "Towards massive machine type communications in ultra-dense cellular IoT networks: Current issues and machine learning-assisted solutions," 2018, *arXiv:1808.02924*. [Online]. Available: http://arxiv.org/abs/1808.02924

DIANA PAMELA MOYA OSORIO (Member, IEEE) was born in Quito, Ecuador. She received the B.Sc. degree in electronics and telecommunications engineering from Armed Forces University (ESPE), Sangolquí, Ecuador, in 2008, and the M.Sc. and D.Sc. degrees in electrical engineering with emphasis on telecommunications and telematics from the University of Campinas (UNICAMP), Campinas, Brazil, in 2011 and 2015, respectively. Since 2015, she has been acting as an Adjunct Professor with the Department of Electrical Engineering, Federal University of São Carlos (UFSCar), São Carlos, Brazil. In 2018, she was a Visiting Researcher with the Centre for Wireless Communications (CWC), University of Oulu, Finland, for one year, where she joined CWC as a Senior Research Fellow under the 6G Flagship Program, in 2020. Her research interests include wireless communications in general, physical layer security, security for 5G and beyond networks, and UAV-based communications. She has served as a TPC and a reviewer for several journals and conferences.

EDGAR EDUARDO BENITEZ OLIVO (Member, IEEE) received the B.Sc. degree in electronics and telecommunications engineering from Armed Forces University-ESPE, Ecuador, in 2008, and the M.Sc. and Ph.D. degrees in electrical engineering from the University of Campinas, Brazil, in 2011 and 2015, respectively. In 2014, he held a Visiting Researcher position with the Centre for Wireless Communications, University of Oulu, Finland. Since 2016, he has been with São Paulo State University (UNESP), Campus of São João da Boa Vista, Brazil, as an Assistant Professor. His research interests include wireless communications, with a current focus on emerging technologies towards 5G wireless networks. He has served as a reviewer for many IEEE and non-IEEE journals and has been involved as a TPC member in several conferences.

HIRLEY ALVES (Member, IEEE) received the B.Sc. and M.Sc. degrees from the Federal University of Technology-Paraná (UTFPR), Brazil, in 2010 and 2011, respectively, in electrical engineering, and the dual D.Sc. degree from the University of Oulu, Oulu, Finland, and UTFPR, in 2015. In 2017, he was an Adjunct Professor of machine-type wireless communications with the Centre for Wireless Communications (CWC), University of Oulu. In 2019, he joined CWC as an Assistant Professor. He is currently the Head of the Machine-Type Wireless Communications Group. He is also actively working on massive connectivity and ultra-reliable low-latency communications for future wireless networks, 5GB and 6G, full-duplex communications, and physical-layer security. He also leads the URLLC activities for the 6G Flagship Program. He was a co-recipient of the 2016 Research Award from the Cuban Academy of Sciences, the 2017 IEEE International Symposium on Wireless Communications and Systems (ISWCS) Best Student Paper Award, and the 2019 IEEE European Conference on Networks and Communications (EuCNC) Best Student Paper Award. He has been the organizer, the chair, a TPC, and a tutorial lecturer for several renowned international conferences. He is the General Chair of the ISWCS'2019 and the General Co-Chair of the first 6G Summit, Levi 2019, and ISWCS 2020.

MATTI LATVA-AHO (Senior Member, IEEE) received the M.Sc., Lic.Tech., and Dr.Tech. degrees (Hons.) in electrical engineering from the University of Oulu, Oulu, Finland, in 1992, 1996, and 1998, respectively.

From 1992 to 1993, he was a Research Engineer with Nokia Mobile Phones, Finland, after which he joined the Centre for Wireless Communications (CWC), University of Oulu. He was the Director of CWC, from 1998 to 2006, and the Head of the Department for Communication Engineering, until August 2014. He has been an Academy of Finland Professor, since 2017. He is currently a Professor of digital transmission techniques with the University of Oulu. His research interests are related to mobile communication systems and currently his group focuses on 5G and beyond systems research.