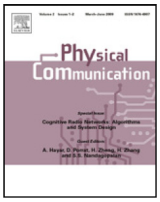
Physical Communication 32 (2019) 1–30

Contents lists available at ScienceDirect

Physical Communication

journal homepage: www.elsevier.com/locate/phycom



Full length article

A survey on OFDM physical layer security

Reem Melki [*], Hassan N. Noura, Mohammad M. Mansour, Ali Chehab

American University of Beirut, Department of Electrical and Computer Engineering, Lebanon

ARTICLE INFO

Article history:
Received 5 June 2018
Received in revised form 13 September 2018
Accepted 25 October 2018
Available online 8 November 2018

Keywords:
Wireless networks
Security
Physical layer
PLS
Security services
Taxonomy

ABSTRACT

Physical Layer Security (PLS) is an emerging paradigm employed to enhance wireless network security without relying on higher-layer encryption techniques. PLS enables legitimate users to exchange confidential messages over a wireless medium in the presence of adversaries, by utilizing the main properties and characteristics of the wireless channel. Traditionally, security in wireless networks has been addressed separately from the physical layer due to its uncontrollable random nature. However, with the massive advances in computational capabilities, classical security techniques are becoming less secure and the need for new schemes is becoming more crucial. As a result, more and more research is directed towards studying, understanding and exploiting the highly random nature of wireless networks. This paper provides a comprehensive survey on various OFDM-based PLS techniques that target popular security services namely, key generation and distribution, data confidentiality, authentication, integrity and availability. With this survey, readers can have a better understanding of the PLS techniques present in the literature, their current limitations, challenges and countermeasures, in addition to future research directions in this area.

1. Introduction

Wireless communication is one of the most pervasive technologies and is, by far, the fastest growing segment of the communications industry [1], with nearly 5 billion users accessing only one array of wireless technologies: cellular communication [2]. Moreover, wireless communication has become crucial for a very wide range of applications including 5G networks, Internet of Things (IoT), Wireless Sensor Networks (WSN), banking, social networking, health monitoring and many others [2]. Orthogonal Frequency-Division Multiplexing (OFDM) has emerged as a promising solution (1) to cope with the ever increasing demand of users and (2) to meet the requirements of next generation networks. The OFDM system possesses several advantages such as high spectral efficiency, strong tolerance to fiber dispersion, flexible resource allocation, low cost and robustness against Inter-Symbol Interference (ISI), among others [3].

1.1. Problem formulation

The broadcast nature of wireless transmission has made this technology vulnerable to passive and active attackers, mainly eavesdroppers who are able to capture, decode and recover the transmitted signals with sufficient power [4]. Conventionally, communication security is viewed as an independent feature and is addressed at the upper layers of the protocol stack by applying traditional cryptographic schemes (data link layer and above) [5]. Some of the well known security protocols are: the Hypertext Transfer Protocol-Secure (HTTPS) which is an adaptation of HTTP for secure communication at the application layer [6], the Transport Layer Security (TLS), which is used to protect the transport layer [7] and the Internet Protocol Security (IPsec), which is designed to secure communication over Internet Protocol (IP) networks [8] (Fig. 1). All of the aforementioned security protocols and the available cryptographic algorithms have greatly improved network security, however, it has always been assumed that the physical layer provides an error-free link, which is not the case in practice. For example, wireless links are more vulnerable to attacks than wired links that provide dedicated channels between users and thus, offer better performance in terms of privacy and security. The security protocols mentioned above operate above the physical layer, which means that the physical layer header is transmitted in plaintext, hence, allowing the eavesdropper to synchronize to the transmitted frames and to possibly recover them. As such, wireless security is still prone to both active and passive attacks since the underlying structures of users' data are not encrypted and are sent in the clear, such as the MAC addresses of the sender and receiver [5]. Moreover, with the emergence of ad-hoc and decentralized networks, upper layer security techniques have become complex and harder to implement. Hence, possible security solutions can be applied at the (1) OFDM level (and its

[*] Corresponding author.
E-mail addresses: rmm71@aub.edu.lb (R. Melki), hn49@aub.edu.lb (H.N. Noura), mmansour@aub.edu.lb (M.M. Mansour), chehab@aub.edu.lb (A. Chehab).

https://doi.org/10.1016/j.phycom.2018.10.008
1874-4907/© 2018 Elsevier B.V. All rights reserved.

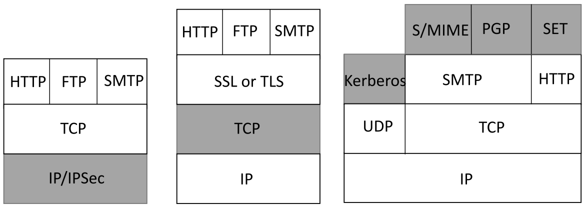


Fig. 1. Traditional security protocols at the network layer, the transport layer and the application layer.

variants) and/or (2) massive MIMO level to re-enforce the security of 5G networks. In this survey, we will be focusing on OFDM-based security solutions.

1.2. Motivation

Motivated by what state-of-the-art wireless technologies have to offer from increased throughput to enhanced resiliency against failures and by the fact that today's wireless networks still suffer from major security vulnerabilities, physical layer security (PLS) has been recently introduced as a promising candidate to ensure the security of wireless communication systems. PLS has received a lot of interest from both academia and industry, and notable progress has been made in terms of (1) understanding the basic physical layer fundamentals and (2) proposing novel ideas and techniques to ensure better wireless network security [9,2,10,11]. Moreover, PLS has the potential to greatly enhance the performance of a very wide range of applications as shown in Fig. 2.

The reason for selecting the physical layer is that it has the least impact on the system and it is the fastest among all layers since it requires only one round of operation when dealing with physical layer signals [12]. The high randomness level of the physical layer is the main motivation behind adopting physical layer security. Additionally, the physical layer is common to all kinds of devices and as such, any security solution at this layer can be useful for all heterogeneous devices. Recently, extensive research work has been presented about the design of wireless PLS schemes [13,14]; many challenging but interesting issues remain open for future contributions. Specifically, existing work in this area focuses on exploring different techniques to establish a first line of defense in security for 5G networks.

1.3. Contribution

The aim of this survey paper is (1) to provide an overview of the recent works done in the PLS area and (2) to provide a thorough understanding and a detailed discussion of the PLS techniques available in the literature. The PLS techniques are divided into five groups:

- Device authentication schemes;
- Key generation and distribution schemes;
- Data confidentiality schemes;
- Source authentication and data integrity schemes;
- Availability schemes.

More specifically, this paper provides a detailed taxonomy of PLS, which is shown in Fig. 3. The contributions of this paper are summarized as follows:

- We present a detailed study on the existing PLS schemes and we categorize them into five groups; each group corresponds to one of the previously mentioned security services. We describe and discuss each technique in a detailed manner for a better understanding of the underlying PLS method.
- We highlight the advantages and weaknesses of each technique and provide ways to overcome the mentioned limitations.
- We summarize the PLS schemes in a tabular form for a side-by-side comparison (Table 1).
- We present a discussion of the research challenges and open problems for PLS that need to be addressed in order to realize its full potential. We also recommend several solutions towards a modern PLS security system.

It should be noted that some PLS techniques in the literature exploit the characteristics of OFDM signals to secure the OFDM system [15,16,9,17,18] while others rely on channel characteristics only [19].

2. Background

2.1. Physical layer as a security solution

2.2. Organization

The rest of the paper is organized as follows (Fig. 4). Section 2 reviews the basic concepts of OFDM systems and briefly explains the types of security services. Section 3 introduces the possible applications of PLS. Section 4 presents the PLS authentication schemes. Section 5 studies the PLS key generation and distribution schemes. Section 6 presents the PLS data confidentiality schemes. Section 7 describes the PLS anti-jamming schemes present in the literature. Section 8 introduces the concept of PLS data integrity and source authentication. Section 9 describes the performance metrics needed to evaluate the security performance of PLS schemes. Section 10 highlights the important conclusions and lessons learned from the work presented in the literature. Section 11 discusses the challenges of PLS schemes presented in the literature and proposes ways to overcome these limitations. Finally, Section 12 concludes the paper.

Due to the fact that signals propagate through air, different kinds of attacks can be performed during wireless transmission. More specifically, some attacks exploit the physical channel characteristics to degrade the performance of wireless communication systems and disrupt their main functionalities. Examples of these attacks are: eavesdropping, jamming, and denial of service (DoS).

Recently, more attention has been drawn to the security of OFDM waveforms with some variants that are expected to ensure a better performance by addressing the weaknesses of OFDM such as the reduced peak-to-average power ratio (PAPR). Note that there have been recent efforts targeting the design of new secure waveforms for future networks other than OFDM waveforms such as the filter bank [43,44].

Since OFDM is currently the most widely used scheme in existing systems, it is expected to maintain its dominance in future systems such as 5G systems [23]. On the other hand, different security requirements are mandatory for 5G systems, some of which are confidentiality, integrity, and availability. The 5G networks have additional and more complex requirements different form previous systems due to the introduction of new techniques and elements such as massive Multiple-Input Multiple-Output systems (MIMO), the filter-bank and many others. Hence, security has become an inevitable requirement for future systems to operate efficiently and they should be addressed at different layers of the protocol stack.

Mainly, there are two approaches to the design of security techniques: (1) computational security and (2) information theoretic security [25]. In computational security, the degree of security of a certain technique is related to the amount of time it takes to break a code [45,46]. Information-theoretic security, on the other hand, does not rely on computational power, but on the

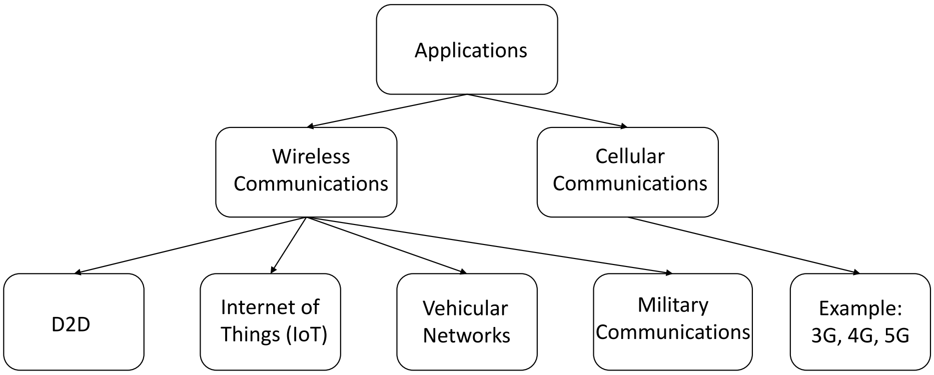


Fig. 2. Digital communication scenarios where PLS is essential.

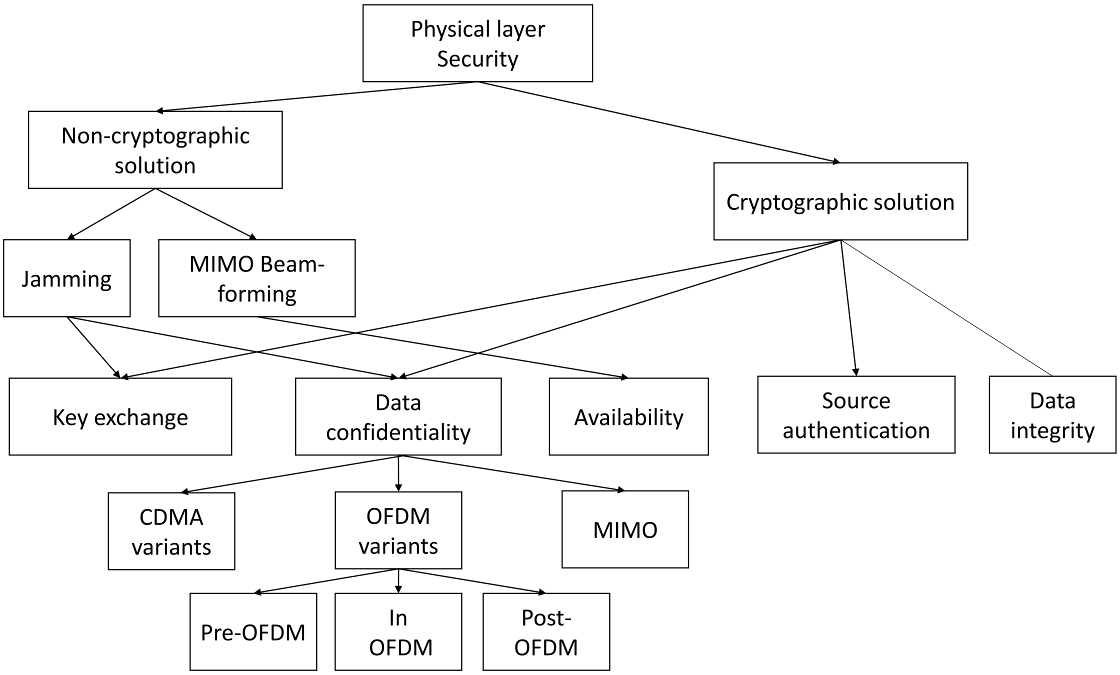


Fig. 3. Proposed PLS taxonomy.

physical properties of the radio channel, and is based on Claude Shannon's early work on the mathematical theory of communication. Shannon's work mainly focused on symmetric key encryption systems [47]. On another note, the work of Aaron Wyner in this field is more relevant to PLS, in which he used the wiretap channel model to prove the idea that secrecy can be attained using the communication channel itself without the need of shared secret keys [48]. Therefore, physical layer security techniques, based on information-theoretic security, have attracted a lot of attention recently [49,50], in which most of the work presented in the literature focuses on maximizing the secrecy capacity, which is an important metric in PLS [25].

Physical layer security methods can be either (1) key-based secrecy [47,51] or keyless security based on Wyner's wiretap channel [48]. While keyless security schemes usually require full or partial channel state information (CSI) of the eavesdropper's channel, which is in most situations unpractical [50], key-based security exploits the randomness of common wireless channels to establish secure keys between two legitimate users. These techniques also require the development of key generation, distribution and management schemes, which can be challenging in today's dynamic and heterogeneous networks.

In [48], the author analyzes the wiretap channel model and proves that a transmitter can send information securely if the signal-to-noise ratio (SNR) of the legitimate receiver is higher than that of the eavesdropper. In this case, the achievable rate is referred to as the secrecy capacity. The model proposed in [48] can be realized when using PLS schemes such as wiretap coding [48,52], beamforming [53], and power allocation [54]. However, in all of the previously mentioned techniques, it is assumed that the transmitter knows the CSI between the eavesdropper and itself, which is rather unrealistic [4].

Therefore information-theoretic physical layer security techniques (OFDM-based) can be divided into four groups [23]:

- **Secret key-based schemes**: Here, the legitimate users first extract a pseudo-random sequence from the channel, and it is only known by these intended users. Then, this sequence is used either to perform data encryption (symbols at the physical layer), dynamic coordinate interleaving or constellation rotation [55].
- **Adaptive transmission schemes**: Transmission parameters are adjusted according to the quality of service (QoS) requirements of the intended receiver. This class of schemes

Table 1
Evaluating data confidentiality techniques.

Reference	Data rate	Security layer	Preamble synchronization	Encrypted data	Computational complexity	Error propagation	Data confidentiality technique
[20]	No loss	Before IFFT	No	Data bits	Assigning distinct phases for each subcarrier	No	Distinct phase for each subcarrier
[21]	No loss	After IFFT	No	Time domain signal	(1) Estimating CSI (2) Estimating total transmit power	No	Cyclic shift
[22]	No loss	Before and after IFFT	Yes	Data bits and training sequence	(1) Generate key (2) Column/row permutation (3) Chaotic subcarrier allocation (4) Chaotic training sequence	Yes	Column–row permutation, chaotic subcarrier allocation, chaotic training sequence
[23]	No loss	Before IFFT	No	Data bits	(1) Estimate CSI (2) Subcarrier interleaving	No	Subcarrier interleaving
[19]	No loss	After IFFT	No	Time domain signal	(1) Estimate CSI (2) Appending AN (3) Jamming	No	AN and Cooperative jamming
[3]	No loss	Before IFFT	No	QAM symbols	(1) Generate pilot cluster using chaotic map (2) OFDM symbol encryption based on chaotic map	Yes	I-phase and Q-phase multiplication by a pair of phase sequences separately
[24]	No loss	Before and After IFFT	No	Data bits and Time signal	(1) XOR operation (2) Multiplying the real and imaginary components of the time domain OFDM samples by two {1,−1} binary key streams	Yes	XOR ENC and Phase ENC
[25]	Loss	Before IFFT	No	Data bits	(1) Estimate CSI (2) Dummy data insertion (3) Pilot design	No	Dummy data insertion
[26]	No loss	Before IFFT	No	Data bits, training symbols and subcarrier	(1) Generate 3 chaotic sequences (2) Chaotic training sequence insertion (3) Chaotic subcarrier masking (4) FrFT operation	No	3D chaotic scheme
[27]	No loss	After IFFT	No	Time domain signals	(1) Secret key sharing (2) Time domain signal scrambling	Yes	Time domain permutation
[28]	No loss	Before and after IFFT	No	Frequency and time signals	(1) Key generation and sharing (2) Frequency and time permutation based on chaotic map	No	Permutation
[29,30]	No loss	After IFFT	No	Time domain signals	Beamforming	No	Beamforming
[31]	No loss	After IFFT	No	Time signal	(1) In the first time slot (2) The source sends wireless energy to power the cooperative jammer, while in the second time slot the source transmits confidential information to the destination	No	Cooperative jamming
[32]	No loss	After IFFT	No	Time domain signal	(1) Estimate optimal transmit power for each subcarrier (2) Allocate subcarrier among multiusers using two auction based algorithms	No	Power allocation
[33]	No loss	After IFFT	No	Time signal	Find subcarrier allocation vector (transmit power vector)	No	Resource allocation
[15]	No loss	Before and After IFFT	Yes	Short training sequence	(1) Embed user-generated bit sequence in STS (2) Modulate bits using a shift in time domain and phase rotation in frequency domain	No	Preamble modulation
[34]	No loss	At IFFT	No	Data bits	(1) Estimate channel (2) Share transform orders (3) Modulate data	No	Data modulation

(continued on next page)

include pre-equalization, power allocation, and fading-based sub-carrier deactivation schemes [56,57].

- **Artificial Noise-based schemes (AN)**: Here, a transmitter designs the AN based on the legitimate receiver's channel and appends it to the transmitted signal in such a way that the eavesdropper is not able to recover the real message.
- **OFDM signal feature suppression**: Such as the concealment of some key features within the OFDM signal.

In the literature, several OFDM-based PLS schemes have been proposed, each addressing one or more of the following security services: (1) mutual device authentication, (2) secret key distribution, (3) session key generation (4) data confidentiality and privacy, (5)

Table 1 (*continued*).

Reference	Data rate	Security layer	Preamble synchronization	Encrypted data	Computational complexity	Error propagation	Data confidentiality technique
[35]	No loss	Before IFFT	No	Data bits	(1) Estimate channel (2) Pre-equalize sent message	No	Channel-based encryption
[16]	No loss	Before IFFT	No	Pilot signal	(1) Estimate channel (2) Manipulate pilot phase and amplitude	No	Pilot Manipulation
[9]	No loss	Before IFFT	No	Data bits	(1) Estimate channel (2) Generate IFFT/FFT blocks based on channel	No	Channel-based encryption
[5]	Loss	Before IFFT	Yes	Data bits and LTS	Generate dummy data and dummy data locations for each symbol (2) Re-arrange LTS to a sequence only known to the legitimate users	No	Encryption using dummy data
[36]	Loss	Before IFFT	No	Data bits	(1) Estimate CSI (2) Data bits are divided in such a way that some are used to derive the active subcarriers indices which will carry the other group of bits (3) Active subcarrier are interleaved based on CSI	Yes	Encryption based on subcarrier index selection
[37]	Loss	Before IFFT	No	Data bits	(1) Estimate CSI (2) Choose active subcarriers accordingly	No	Encryption based on subcarrier index selection
[4]	No loss	After IFFT	No	Time domain signal	(1) Estimate CSI (2) Artificial noise is added	No	Artificial noise
[38]	No loss	Before IFFT	No	Data bits	(1) Real and imaginary axes of a subcarrier symbol are interleaved	No	Permutation
[39]	No loss	Before IFFT	No	Data bits	(1) Estimate CSI (2) Pre-compensate CFO before transmitting	No	CFO pre-compensation
[40]	No loss	Before and after IFFT	No	Data bits	(1) Generate and share a secret key (2) Interleave both the frequency and time information using a chaotic map	Yes	Interleaving
[41]	No loss	Before IFFT	No	Data Bits	Use imaginary part of the symbol as an encryption key	No	Data encryption
[42]	Loss	After IFFT	No	Time domain signal	(1) Jam the time domain signal (2) Estimate the jamming signal to recover data	No	Jamming

data integrity and source authentication and (6) availability. Each of the mentioned security services will be defined and discussed separately in Section 2.3.

Moreover, it should be noted that when assessing and analyzing a specific security solution, we will focus on the following points:

- Low computational complexity and hence, low latency.
- Low resource requirement (especially for devices with limited battery such as mobile phones or sensors).
- High level of security.
- Minimum communication overhead (minimizing the side information).

2.3. *Security services*

In the general sense, information security is related to confidentiality, integrity and availability (Fig. 5).

Basically, data confidentiality is information/data secrecy. It is the prevention of unauthorized disclosure (access) to sensitive information [58–61]. Usually, data confidentiality is ensured through encryption, mainly symmetric encryption since it is more efficient than asymmetric encryption, which is typically used for exchanging session keys.

Data integrity, on the other hand, validates that the sent data has been received as is and that no modification or alteration has been done by unauthorized users. Hashing is a one-way operation that ensures data integrity.

In addition to the two security services presented above, maintaining communication availability is crucial since users should be able to access information at all times. Adversaries try to interrupt the availability of information through denial of service (DoS) or even distributed denial of service (DDoS), which can be detected and prevented using intrusion detection/prevention systems or Security Information Event Management (SIEM) [62].

Authentication, which is also essential, is another security service and it is about verifying the legitimacy (identity) of the communicating parties using cryptographic protocols.

Adversaries seek to breach security through disclosure, alteration, or denial of service. Hence, cryptographic or non-cryptographic algorithms are required to guarantee a good security level.

On the other hand, encryption algorithms may operate at the block level or stream level. While a block cipher divides the data into blocks of fixed sizes (usually 128 bits), a stream cipher processes data bit-by-bit and mixes it with a pseudo-random stream [61].

Additionally, most cryptographic algorithms apply the same round function several times in order to ensure two essential properties, Confusion and Diffusion. The former obscures the relationship between the used secret key and the ciphertext, while

- ➢Introduction
  - Problem formulation
  - Motivation
  - Contribution
  - Organization
- ➢Background
  - Physical Layer as a Security Solution
  - Security services
  - OFDM and its variants
- ➢PLS and its Possible Applications
  - Device-to-Device (D2D)
  - Internet of Things (IoT)
  - Vehicular Communications
  - Femtocells
- ➢Device authentication schemes
- ➢Key generation and distribution schemes
- ➢Data confidentiality techniques
  - Data confidentiality schemes
    - Permutation
    - Phase encryption
    - Channel-based data encryption
    - Artificial noise and artificial fast fading
    - Preamble encryption
    - Power allocation
    - Jamming-based encryption
    - Joint PLS enhancement and PAPR reduction
  - Channel and hardware impairments
  - Performance and robustness evaluation of existing cipher approaches
- ➢Existing anti-jamming PLS solutions
- ➢ Source Authentication and Data Integrity Techniques
- ➢Performance metrics
- ➢Lessons
- ➢Discussion
- ➢Conclusion

Fig. 4. The structure of the article.

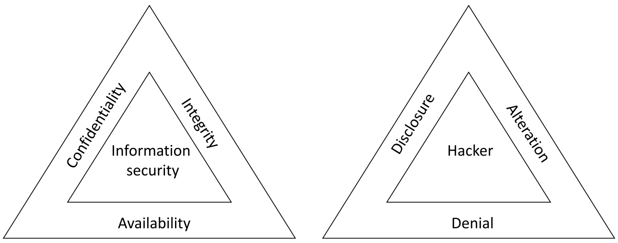


Fig. 5. The classical models of information security principles.

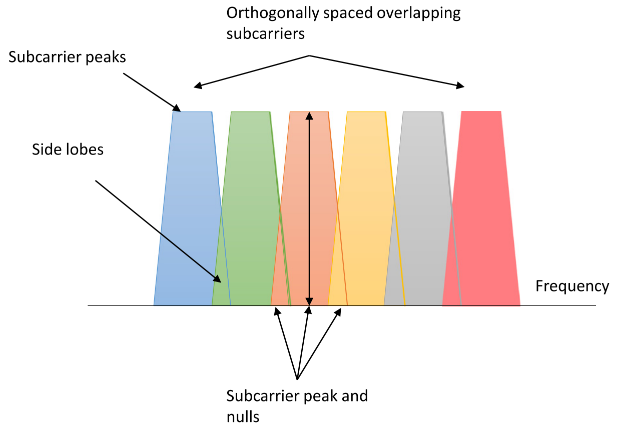

Orthogonally spaced overlapping subcarriers
Subcarrier peaks
Side lobes
Frequency
Subcarrier peak and nulls

Fig. 6. OFDM frequency spectra.

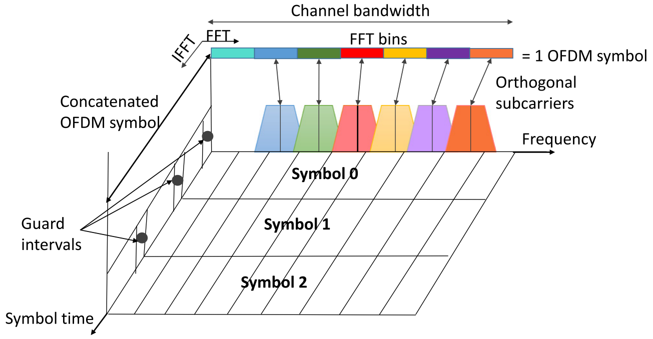


Fig. 7. OFDM representation in time and frequency domains.

the latter guarantees that a change in a plaintext symbol affects several ciphertext symbols [59].

2.4. OFDM and its variants

In this section, we introduce a general overview of the basic concepts of OFDM and its variants, which are necessary for the fundamental understanding of the PLS techniques discussed later in this paper.

2.4.1. OFDM

Orthogonal Frequency Division Multiplexing (OFDM) was first introduced in the late 1950's [63,64]. Since then, it has been widely adopted as the basic building block for many current modulation schemes in different technologies such as 802.11 WLAN, 802.16 WiMAX, and 3GPP LTE. In principle, the frequency band is divided into multiple narrower sub-bands, each modulated with a conventional digital modulation scheme. The large number of closely-spaced overlapping sub-carriers, transmitted in parallel, leads to an increase of the spectral efficiency (Fig. 6). This is one of OFDM's main advantages. Another advantage is overcoming the effect of frequency selective fading, which results from multi-path propagation [65]. This requires each sub-band to have a bandwidth satisfying [66]:

$$B < \frac{1}{2\pi\,\tau_{avg}}, \tag{1}$$

where τ_{avg} is the average delay spread. Therefore, the problem of having a frequency selective fading channel is simplified to having multiple flat fading sub-channels which can be easily mitigated by equalization.

Another issue in OFDM is Inter-Symbol Interference (ISI) and Inter-Carrier Interference (ICI). ISI is the interference caused by adjacent symbols due to the delay spread (τ), while ICI is interference caused by adjacent sub-carriers. To overcome ISI and ICI, a guard interval, also known as cyclic prefix (CP), is inserted between consecutive OFDM symbols and its length is set to be more than the channel delay spread. The cyclic prefix is simply an extension of the signal itself appended at the beginning of the OFDM symbol [67].

Fig. 7 illustrates the main concepts of an OFDM signal, which is represented in both time and frequency domains. Conceptually, a combination of Fast Fourier Transform (FFT) and Inverse Fast Fourier Transform (IFFT) digital signal processing is required for OFDM implementation. These transforms are important from the OFDM perspective because they can be viewed as mapping digitally modulated input data (data symbols) onto orthogonal subcarriers [67–69]. Figs. 8 and 9 show the detailed OFDM transmitter and receiver block diagrams, respectively.

OFDM is adopted in the IEEE 802.11 a/g/n standards for signal modulation [70]. The corresponding structure of the physical layer packet of IEEE 802.11 OFDM is shown in Fig. 10. The packet consists

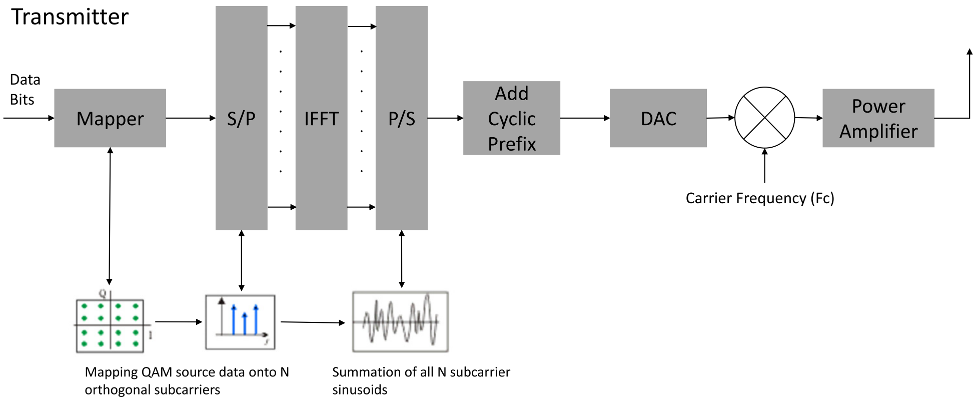


Fig. 8. A detailed OFDM transmitter block diagram.

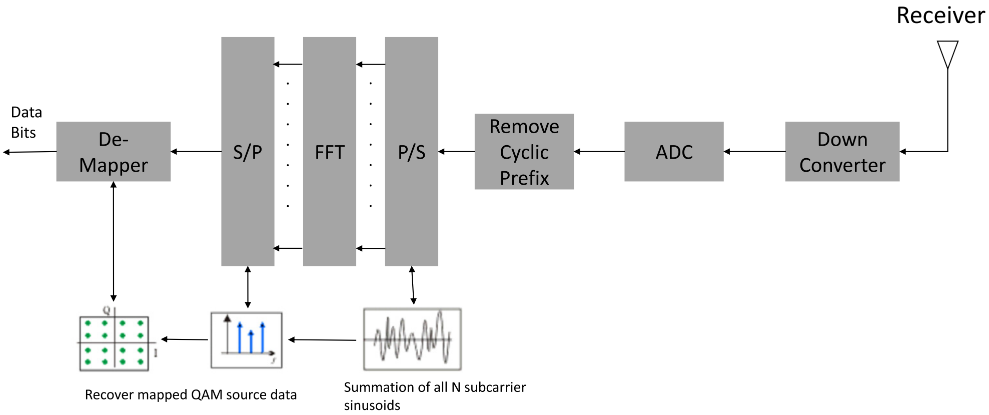


Fig. 9. A detailed OFDM receiver block diagram.

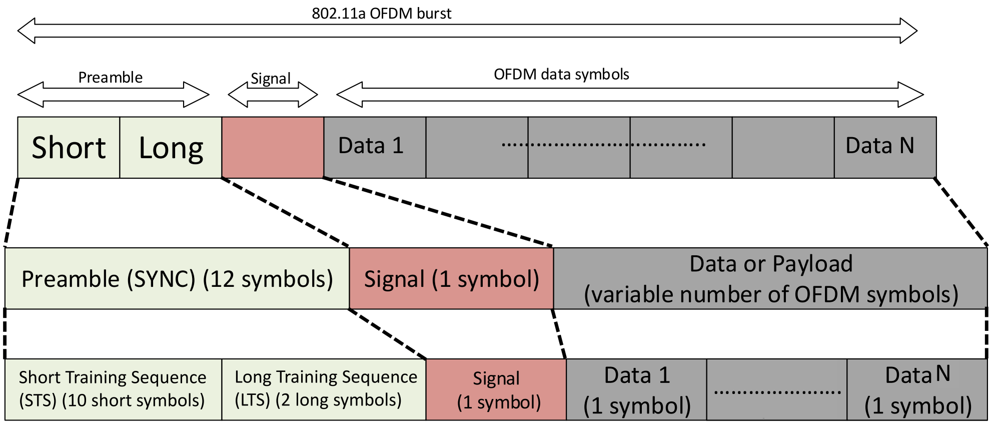

802.11a OFDM burst
Preamble
Signal
OFDM data symbols
Short
Long
Data 1
Data N
Preamble (SYNC) (12 symbols)
Signal (1 symbol)
Data or Payload (variable number of OFDM symbols)
Short Training Sequence (STS) (10 short symbols)
Long Training Sequence (LTS) (2 long symbols)
Signal (1 symbol)
Data 1 (1 symbol)
Data N (1 symbol)

Fig. 10. 802.11a frame structure.

of a preamble, a SIGNAL field and a DATA (payload) field [11]. The DATA field includes the transmitted data bits. The SIGNAL field, which is equivalent to one OFDM symbol, carries information related to the coding rate, the mapping scheme and the length of the DATA field. The preamble, on the other hand, is 16 μs long and is divided into two fields: the short training sequence (STS) field and the long training sequence (LTS) field (Fig. 10) [11,15].

- **STS Field**: Consists of ten repetitions of STS, each having a duration of 0.8 μs. The STSs are mainly used for signal detection, coarse frequency offset estimation, automatic gain control (AGC) diversity selection and time synchronization [67].
- **LTS Field**: Includes a guard interval (1.6 μs) and two repetitions of LTS (3.2 μs each). The LTSs are used for channel estimation (CSI), fine frequency offset estimation and channel equalization [67].

2.4.2. *OFDM Variants*

The CP in OFDM introduces redundancy in transmitted signals and degrades the overall performance in terms of data rate, spectral and power efficiency [71]. Additionally, OFDM systems suffer from two major drawbacks which are: (i) high Peak-to-Average Power Ratio (PAPR) and (ii) high Out-of-Band (OOB) emissions. Basically, all Multi-Carrier Modulation (MCM) waveforms experience high PAPR, however, frequency confinement varies significantly from one MCM waveform to another. OFDM uses a rectangular pulse shape which results in poor confinement in frequency domain leading to high OOB emission [72].

This has lead to the emergence of other MCM methods, mainly the Filter Bank Multi-Carrier transmission scheme (FBMC), the Universal Filter OFDM (UF-OFDM) and the Generalized Frequency Division Multiplexing (GFDM) as promising candidates for the future 5G mobile communication systems. These methods will be briefly discussed below:

- **FBMC:** This technology eliminates the CP and introduces filter banks to the OFDM system. FBMC is one of the key technologies of future networks: 5G networks. The FBMC has been designed to overcome the drawbacks of OFDM systems and to enhance the system's performance, efficiency and flexibility. More Specifically, instead of using a CP, FBMC uses an array of filters equal to the number of sub-carriers (sub-carrier level) and OQAM (offset QAM) modulation to reduce the out-of-band power leakage and increase the spectral efficiency with low costs [73].
- **UF-OFDM:** UFMC group's subcarriers to sub-bands (subgroups) and then applies filtering to each subgroup separately. Hence, UFMC can be seen as a compromise between OFDM and FBMC since it requires less overhead and low complexity compared to FBMC [74].
- **GFDM:** GFDM also uses the filter bank multi-carrier concept. Basically, GFDM spreads the available spectrum for each user into multiple spectral segments, each having more or less bandwidth [74].

It should be noted that this survey targets OFDM-based security solutions since the majority of the work in the literature is in this field and very minimal work tackles the security of other variant systems. However, any of the presented techniques can be adapted and integrated into any of the OFDM-variant systems.

3. PLS and its possible applications

In order to highlight on the importance of PLS in OFDM systems, several emerging technologies (which are based on OFDM) are presented next. It should be noted that PLS can be applied to all types of applications (Machine-to-Machine (M2M), Point-to-Point or Link-to-Link), especially those adopting wireless communications.

M2M is a generic class of applications in which a variety of devices communicate with each other or through a network. More specifically, it refers to the communication of machines (objects) with each other, directly [75]. In what follows, state-of-the-art technologies that fall under "Machine-to-Machine (M2M) communications" are listed and discussed briefly.

3.1. Device-to-Device (D2D)

Recently, D2D communications have attracted a lot of research attention since it enables the development of efficient solutions for direct communications between two devices.

Device to Device (D2D) communication is one of the key components of 4G/5G networks. Basically, D2D improves network capacity and enables mobile devices to communicate directly without referring to the base station, as shown in Fig. 11.

However, one of the major issues in this technology is its security, which needs to be investigated and enhanced, since the propagation medium is vulnerable to different kinds of attacks [76].

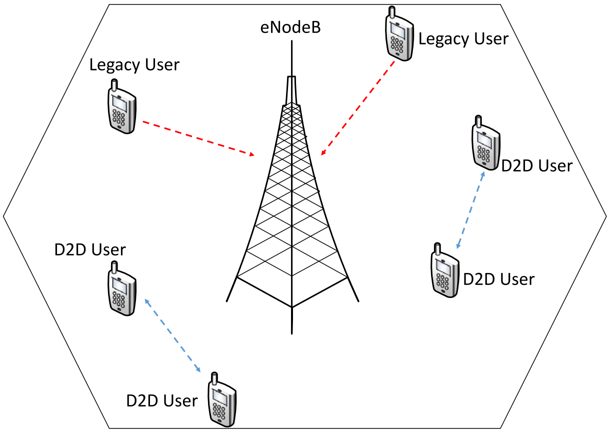


Fig. 11. D2D communication systems.

3.2. Internet of Things (IoT)

The Internet of Things (IoT) is a network of Internet-connected devices (objects) that are able to monitor, access, collect, exchange and evaluate data without human-to-human or human-to-computer intervention. (Fig. 12). Moreover, IoT has become the building block for many services, some of which are: smart houses, smart cities, smart buildings, health monitoring and traffic monitoring [77].

On the other hand, IoT suffers from many security and privacy issues since it is vulnerable to a wider range of threats compared to traditional networks. Having "everything" connected in IoT is both, an advantage and a disadvantage. The main advantage is being able to control all kinds of (connected) devices remotely. However, this control should be restricted to authorized personnel only, otherwise adversaries would be able to gain access to sensitive information and conduct malicious attacks (eavesdropping, inserting, modifying and deleting packet contents). Therefore securing IoT networks is inevitable and mandatory.

3.3. Vehicular communications (V2X)

The major advances in wireless communications and the "Internet" have paved the way for many technologies that were considered impossible and futuristic, few decades ago. These technologies have been considered revolutionary since the human lifestyle has been affected and improved drastically. Examples of such technologies are: health monitoring, smart cities and Intelligent transportation systems (ITS). The latter has become an important research field since it ensures and enhances road safety and creates efficient traffic conditions. ITS is based on vehicular communication, which is known as Vehicular Ad hoc NETworks (VANETs). Vehicular communication (V2X), in turn, is divided into three kinds: vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and Infrastructure-to-Infrastructure (I2I) communications (Fig. 13). Consequently, enhancing the security of V2X is directly related to ensuring the safety of drivers and passengers, which is important and cannot be compromised [78].

3.4. Femtocells

The field of wireless mobile telecommunications has evolved dramatically due to constantly increasing demand (bandwidth) of mobile users (3G, 4G, 5G). One way to provide a higher throughput and to enhance performance is by increasing the number of small base stations such as femtocells. Unlike other small base stations such as microcells, picocells or relays, which are directly connected

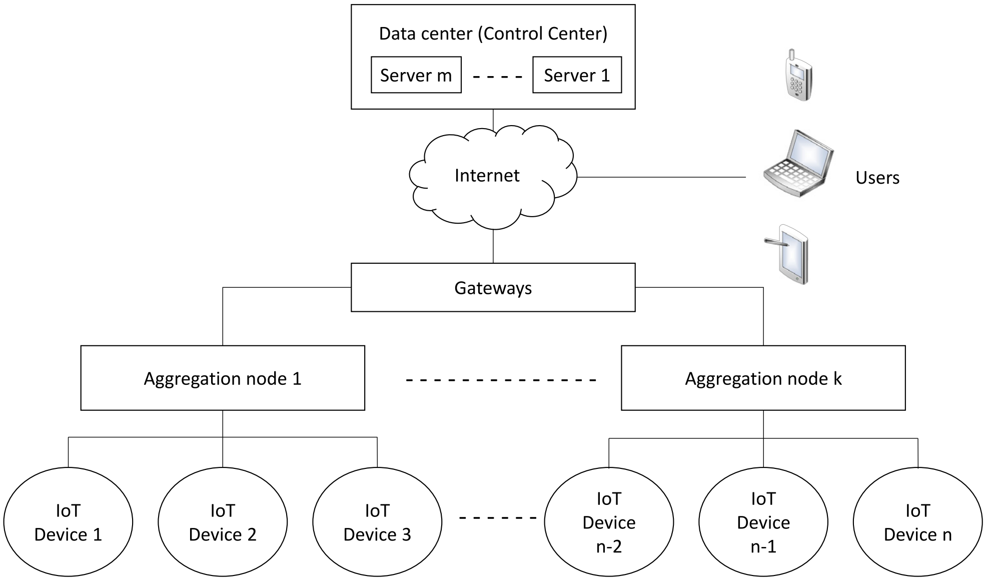


Fig. 12. Internet-of-Things block diagram with n IoT devices, k aggregation nodes and m servers.

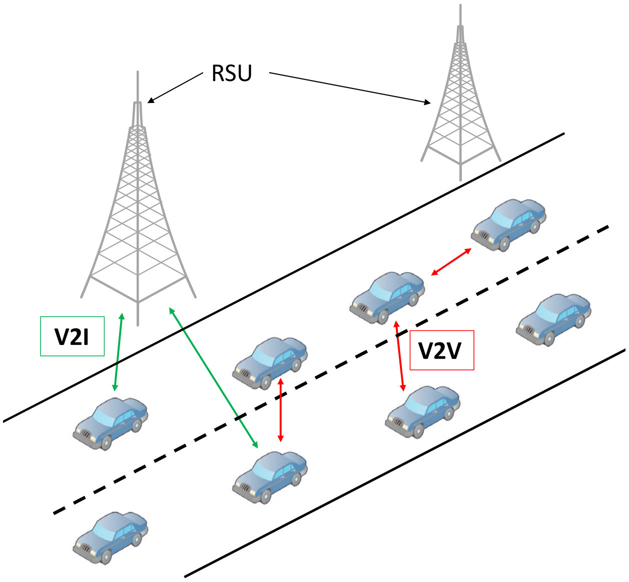


Fig. 13. V2X communication systems.

to the home base station via radio interface, femtocells are connected to the mobile core network via a broadband connection such as DSL or fiber optics. Femtocells are mostly located within indoor environments and are thus, accessible by any individual. As a result, these cells and their base stations are victims of many security threats and attacks [79].

4. Device authentication schemes

Typically, in key-based authentication, the transmitter sends a random number as a challenge, and the receiver sends back the hash of both the shared key and the challenge, or the transmitter encrypts a random number or nonce using the secret key and the receiver sends back the random number incremented or a function of the nonce, both encrypted using the secret key.

Recently, several physical layer authenticating schemes have been proposed for authenticating the transmitter and receiver at the physical layer. These schemes can be classified as keyless or key-based authentication schemes. The former exploits specific features of legitimate devices or specific features of the shared channel between the users. However, this technique is considered difficult and weak since there should exist some level of trust between any two users in order to share and identify the features used in authentication and hence, this approach cannot be considered as a secure device authentication scheme. As such, to achieve the required security level, a secret key should be introduced. This is more practical and closer to the traditional challenge-response mechanism in which authentication is based on both a secret key shared between users, and the channel characteristics [14].

Since the PLS authentication mechanisms, which rely on the characteristics of the shared channel, are considered vulnerable, several papers in the literature proposed adding other variables to the channel characteristics to strengthen the authentication mechanisms against malicious attacks. In [14], the authors propose an enhanced version of the scheme presented in [80], in which Tikhonov-distributed artificial noise is added to interfere with the phase-modulated key that will be used in the authentication process. Similarly, the authors of [81] integrate multipath delay characteristics to the channel impulse response for authentication.

The research presented in [82] experimentally investigates the carrier frequency offset (CFO) monitoring as an authentication method. Assuming the two users (A and B) are communicating, users' authentication is verified if the following condition holds:

$$|\Delta CFO_{AB}| = |\Delta CFO_{BA}| \quad (2)$$

The Time Bounded Anti-Spoofing (TBAS) technique is presented in [83] to enhance Wi-Fi authentication. Specifically, this technique leverages the CSI of the shared channel for the purpose of mutual authentication. Moreover, this technique is based on the facts that (1) different transmitting locations will likely result in different wireless channels, and (2) the channel state drift within a short time interval should be bounded. The proposed authentication method works as follows: the receiver continuously estimates the CSI upon the reception of a new packet. If, within a short period of time, the difference between the channel state of two consecutive packets having the same address is large, then, the receiver concludes that one of these packets is spoofed and hence drops them. This is similar to the authentication mechanism presented in [84].

In [85], the authors explore the potential possibility of using physical-layer channel responses as authenticators between each communicating pair. The proposed authentication scheme, Physical layer Assisted Authentication (PAA) for VANETs (Vehicular Ad hoc Networks), exploits the advantage of having unique Physical layer (PHY) channel responses for each communicating pair such that the receiver would be able to identify the transmitter. More specifically, the sender appends the channel response estimated at its side, which is referred to as the authenticator signal, with the transmitted data. Consequently, the receiver authenticates the sender by comparing the authenticator signal with the estimated channel response at its side. If the two are close, then the sender is authenticated, otherwise the message is ignored. The same concept is applied in [86]. Similarly, in [87], the receiver can also compare the channel matrices of two consecutive frames; if the difference is small, then the sender is authenticated; if the difference is larger than a predefined threshold, then the communication is terminated.

Differently, the authors in [88] proposed a distributed authentication model in which several receiving nodes and a third party authority are involved. Whenever a receiving node estimates the channel response, it relays the information to the third party authority, which is responsible for the decision making (authentication of users).

The authors of [89] proposed *PriLA*, PRIvacy-preserving Location Authentication systems in OFDM based Wi-Fi networks: First, the mobile user and the location-based service (LBS) provider exchange handshake frames and extract both the CSI and the CFO information, which will be used to generate the secret for the encryption of the following frames. Upon receiving the encrypted frames, the LBS provider performs decryption and extracts the user's MAC address and location information. Then, the LBS provider uses the CSI obtained from the received frames to construct a multipath profile, which is compared to the already stored profiles. Accordingly, the LBS provider authenticates the sender and delivers the service.

Authors in [90], on the other hand, consider a two-hop wireless network that involves a relay and present two physical layer challenge-response authentication mechanisms. These mechanisms require a random number, channel finding, channel reciprocity and a pre-shared secret key. In the first mechanism, which assumes that the relay is trustworthy, the sender first generates a random number, n, and sends it to the relay, which forwards the signal to the receiver. The receiver calculates the inverse of the received signal and multiplies the result with a shared key, K, and sends the obtained signal to the relay. The relay in turn forwards the received signal back to the sender. Having n and K, the sender can authenticate the receiver. The protocol is depicted below:

- node B | sent message: Request → Relay (R) → node A | received message: Request
- node A | sent message: n → node R | received message: nH_{AR}
- node R | sent message: nH_{AR} → node B | received message: $nH_{AR}H_{RB}$
- node B | sent message: $K/nH_{AR}H_{RB}$ → node R | received message: K/nH_{AR}
- node R | sent message: K/nH_{AR} → node A | received message: K/n

where H_{ij} is the channel between nodes i and j.

An obvious weakness of this protocol is that the relay, or even an eavesdropper, are able to obtain the secret shared key K by simply multiplying the first signal with the second one. The second mechanism assumes that the relay is not trustworthy, and thus, it is more complicated and can be summarized as follows: the sender generates a random number, n, and sends it along with the first shared key K_1 as two different OFDM symbols. The relay forwards the signal to the receiver, which divides the two signals and extracts the random number, having K_1. Afterwards, the receiver sends the extracted random number and another shared key K_2 as two different OFDM symbols to the relay, which forwards them to the sender. The same operation is done at the sender's side to extract the random number and thus verify the receiver. This technique requires not one, but two secret keys between users. Moreover, messages are sent in plaintext, which will allow the eavesdropper to extract the random number and the secret keys. The detailed procedure is shown in Fig. 14 and is illustrated below:

- node B | sent message: Request → Relay (R) → node A |received message: Request
- node A | sent message: $[K_1, n]$ → node R | received messages: $[K_1H_{AR}]$ and $[nH_{AR}]$
- node R | sent messages: $[K_1H_{AR}]$ and $[nH_{AR}]$ → node B | received messages: $[K_1H_{AR}H_{RB}]$ and $[nH_{AR}H_{RB}]$
- node B | sent message: $[K_2, n]$ → node R | received messages: $[K_2H_{RB}]$ and $[nH_{RB}]$
- node R | sent messages: $[K_2H_{RB}]$ and $[nH_{RB}]$ → node A | received messages: $[K_2H_{BR}H_{RA}]$ and $[nH_{BR}H_{RA}]$

The authors of [91] use the concept of fingerprint embedding for message and user authentication. Here, it is also assumed that there exists a secret key between legitimate users. First, the sender generates a "tag" from the secret key and the data, and superimposes the resulting tag onto the modulated message. At the receiver side, the data is estimated first and then, using the secret key, encrypts the recovered data. The resulting cipher-text is compared to the sent tag, and if there is match, then the sender is authenticated.

The technique presented in [92] is similar to the one discussed previously expect that the tag is generated from the message, S, and the secret, K, via a keyed-hash (MAC) operation. After generating the tag, the sender appends the tag to the message, S, and sends it to the receiver which, in turn, extracts the message, performs hash using K and compares the generated hash to the one generated by the sender. Similarly, the techniques in [93] and [94] use the concept of "tags". However, the tags, which are generated using a secret key, are appended to the payload of the modulated signal, and then, the result is sent to the receiver, which extracts the payload, generates the tag and compares the generated tag to the sent one.

The concept of hashing is also used in [95]. User B sends a random signal to User A, who estimates the channel and generates a hash using the response of the multi-path channel and the secret key. The resulting hash is then sent to B, who estimates the channel and also generates a hash in a similar manner to A and compares the two hashes.

Finally, a pilot authentication scheme for a two-user multi-antenna OFDM system, is presented in [96]. It is based on the "Code-Frequency Block Group (CFBG)" coding mechanism, in which sub-carrier blocks are (1) encoded to authenticate pilots and (2) reused for channel estimation.

Fig. 15 and Table 2 summarize the techniques used in physical layer security for device authentication. Table 2 also presents the advantages, limitations, complexity and cost of each of the presented schemes.

5. Key generation and distribution

Key generation and distribution schemes are divided into: (1) Keyless Security and (2) Secret Key-based Security [97] (Fig. 16). While keyless Security requires no shared keys between the communicating entities, legitimate users should have partial/full knowledge of the eavesdropper's CSI, which is considered very complex in terms of implementation and rather impractical. Secret Key-Based Security, on the other hand, is further discussed

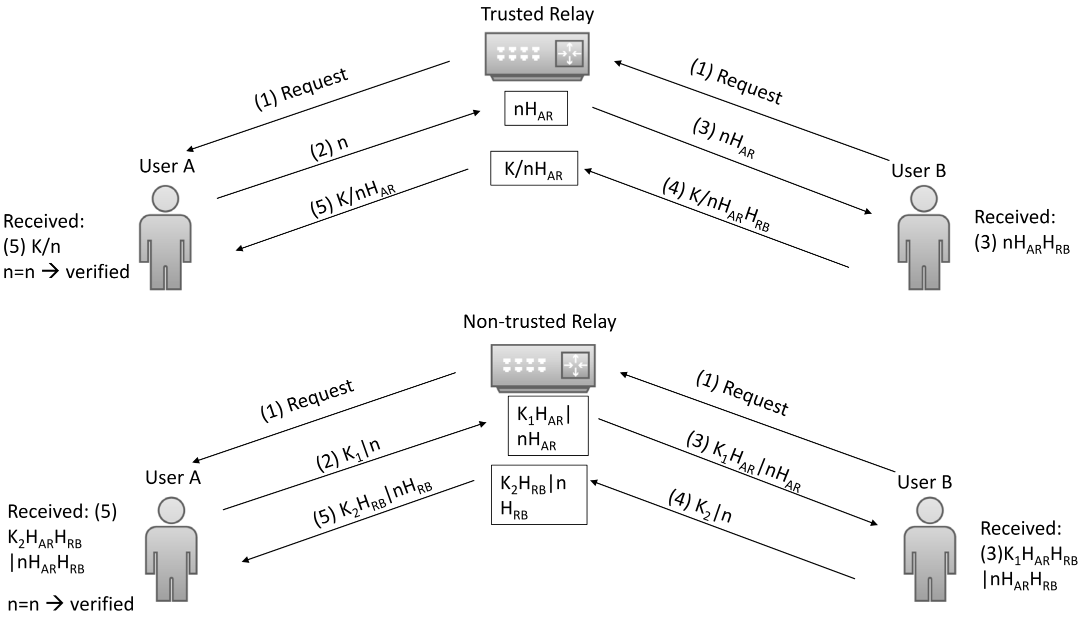


Fig. 14. The authentication scheme presented in [90].

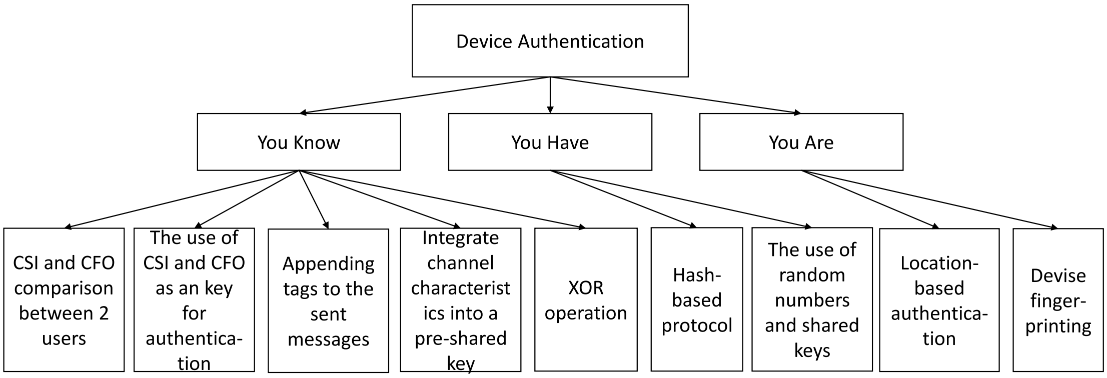

Device Authentication
You Know
You Have
You Are
CSI and CFO comparison between 2 users
The use of CSI and CFO as an key for authentication
Appending tags to the sent messages
Integrate channel characteristics into a pre-shared key
XOR operation
Hash-based protocol
The use of random numbers and shared keys
Location-based authentication
Devise finger-printing

Fig. 15. Proposed device authentication classification used in PLS.

Table 2
A summary of the PLS device authentication schemes.

Device authentication schemes	Comparison of the channel properties of two consecutive frames (CSI,CFO)	Third party authority (relay) using XOR and simple multiplication operations	Using secret keys derived from the channel for encryption	Concept of "tags" which can be generated using encryption or hashing
Advantage	No additional cost and overhead	Non-repudiation	Utilizing the notion of a secret key	Utilizing the notion of a secret key
Limitation	Ineffective when attacker is near legitimate user, that is when both experience same channel conditions	The third party authority is vulnerable to being impersonated. Moreover a high level of trust should exist between legitimate users and the third party	A secret key derived from the channel is a weak proposition since it can be easily generated and acquired	Computationally complex. It requires additional operations at the transmitter and receiver
Resource and communication cost	No additional cost and overhead	Authentication is verified through multiple rounds of communications (3 rounds) and performing simple operations such as XORing	Two steps are done prior to data transmission: (1) Key extraction. (2) Encryption and decryption operations are performed	(1) Key extraction and (2) "tag" generation. (3) Append "tags" to the transmitted messages
Complexity	Not computationally complex: performing comparison	Not computationally complex: performing XOR operations	Computationally complex: encryption	Computationally complex: encryption

throughout this section due to its inevitable importance to PLS and due to the many research advances in this field.

Note: In theory, channel reciprocity is the same frequency spectrum shared by the uplink and downlink. It is also when the

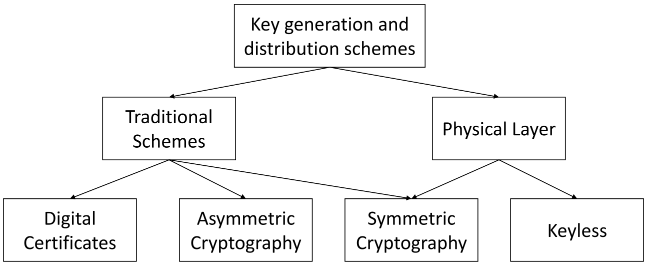


Fig. 16. General classification of key generation and distribution techniques.

coherence time of the channel is greater than the OFDM packet period, which is the case of a channel with low doppler spread [67].

5.1. Key generation and distribution schemes

In network security, major emphasis is targeting key generation and distribution (public, private and session keys) [98] due to its importance in many applications such as IoT, D2D and military communications where security is crucial (Section 3). However, with the emergence of PLS, active research has shifted towards finding alternative techniques to public key cryptography where two users are able to exploit the un-predictable characteristics (randomness) of their shared wireless channel to generate a symmetric session key. This technique is low cost and simple, and exploits the most important feature in the physical layer, randomness, as the building block of the generated encryption/authentication key [99]. Theoretically, a low-randomness key will compromise the security of the system due to the small search space when conducting brute force attacks. Several techniques related to this issue are introduced and further discussed in this section.

Assumption: In the following techniques, legitimate users are considered to be $\frac{\lambda}{2}$ away from each other so that channel reciprocity is ensured, and the eavesdropper is considered to be at a distance $> \frac{\lambda}{2}$.

A straightforward method for generating shared session keys is to extract them from the CSI directly. Such a scheme is presented in [100] where legitimate users exchange several dummy data packets, N, and for each received packet, the CSI is extracted and stored in a matrix. The columns of the matrix correspond to the sub-carrier index on which the packet was sent and the rows correspond to the packet number. Afterwards, the CSIs of each packet in a single column are checked; if the CSIs are in ascending order, one bit in the secret key is set to one otherwise, it is set to zero. Hence, the secret key between two users is constructed without exchanging any information publicly.

Similarly, the approach presented in [101] includes the following four phases: channel estimation, public discussion, secret key extraction and verification. The key is directly generated from the channel frequency response of the legitimate users as shown in Fig. 17. This technique is simple but not fully secure since the generated key solely depends on the channel between the two parties, which is accessible by others (attackers and eavesdroppers).

Moreover, the authors of [99] use the same concept above, exploiting channel randomness via extracting the CSI. However, the keys are extracted from the channel responses of individual OFDM sub-carriers over time. The paper also provides a thorough theoretical modeling of the system and channel, which will lead to the optimal probing rate and maximal key generation rate KGR.

Another simple technique is introduced in [102], where two legitimate users exchange data to estimate the channel between them. Then, a transmitter pre-equalizes the sent message, which contains the secret key. This technique decreases the probability of an eavesdropper intercepting the transmitted signal while perfect decoding can be done at the receiver's side only (Fig. 18). The technique is simple and requires no further action at the receiver's side, however, in case the eavesdropper is able to retrieve the secret information from the shared channel between users, she will be able to recover the real data.

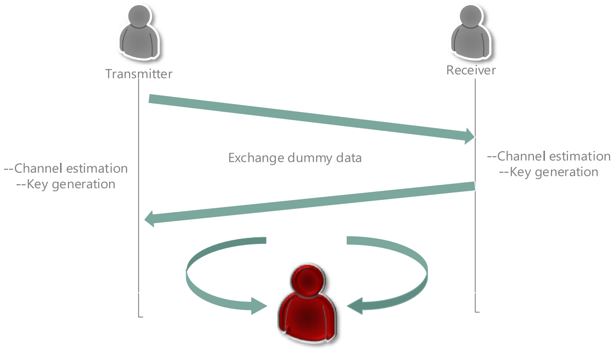


Fig. 17. Key generation method based on channel estimates [101].

In [103], the authors use a new mechanism for generating encryption keys. The keys are obtained from the bipolar real OFDM samples at the output of the optical OFDM systems: the transmitter multiplies the OFDM symbol (S_0), from which the initial session key (K_0) will be derived, with a key only known to the transmitter (g_{TX}). The output is sent to the receiver, which multiplies the received signal with its own key (g_{RX}) and re-sends the result, $((S_0).*(g_{TX})).*(g_{RX})$, to the transmitter. Again, the transmitter multiplies it with its own key (g_{TX}), which results in: $(S_0).*(g_{RX})$; this is sent to the receiver, which will in turn multiply with its key to recover S_0 and then extract K_0. The multiplication procedure mentioned in this technique refers to the element-wise multiplication operation. K_0 is only used for the encryption of the first bipolar OFDM signal. The following encrypted signals $\hat{S}_{i+1}$ are encrypted with K_i, which is obtained from the cyclic prefix of the previous signal, S_i. The cyclic prefix is a copy of the last samples of the data included in the payload. The weakness of this technique is depicted in Fig. 19.

Differently, authors in [104] exploit the inherent randomness that exists within an integrated circuit (such as an FPGA or RFID chip) [105,106] to implement a PLS scheme based on Physical Unclonable Functions (PUFs). Optical scattering-based PUF devices, on the other hand, are primarily used for creating identification and authentication keys [107,108]. The mechanism aims to generate a secret session key used for encryption and it is shown in Fig. 20 and behaves as follows: the transmitter (user A) and receiver (user B) connect their devices and each one generates an equal number of optical scattering-based communication PUF (CPUF), N, using N input spatial light modulator (SLM) pattern which illuminates a volumetric scattering medium with a random coherent optical wavefront. Each combination of K(A)⊕K(B) (key-mixture) is saved in a digital electronic dictionary corresponding to all SLM patterns. The dictionary is assumed to be public and available to all devices locally. Afterwards, whenever a secure message is sent to B, A picks a key k(A) from the cluster which contains all available pre-generated keys and XORs this key with the message. B receives the encrypted message and generates both the key-mixture and k(B) to recover the original message. The key-mixture will eliminate k(A), and k(B) will cancel itself, thus, obtaining the message. In this technique, A sends the XORed message and the corresponding pattern, P_i, in order to help user B recover the message. However, with the key-mixtures and the $P_i s$ publicly available, any eavesdropper is able to break this system using the chosen ciphertext attack.

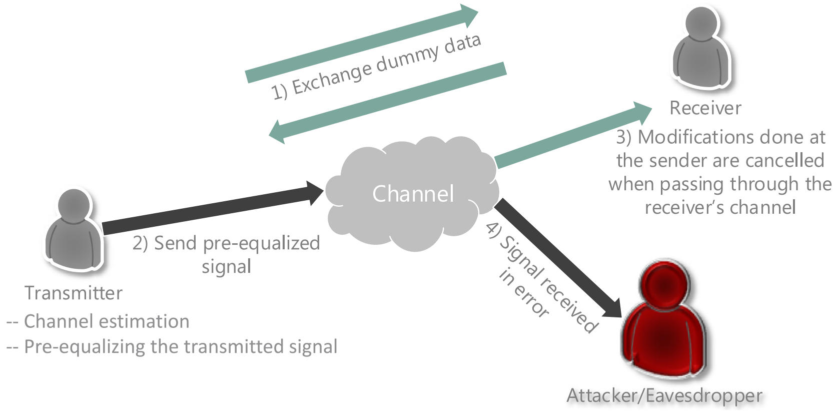

1) Exchange dummy data
Receiver
3) Modifications done at the sender are cancelled when passing through the receiver's channel
Channel
2) Send pre-equalized signal
4) Signal received in error
Transmitter
-- Channel estimation
-- Pre-equalizing the transmitted signal
Attacker/Eavesdropper

Fig. 18. Key distribution method based on pre-equalization/pre-coding [102].

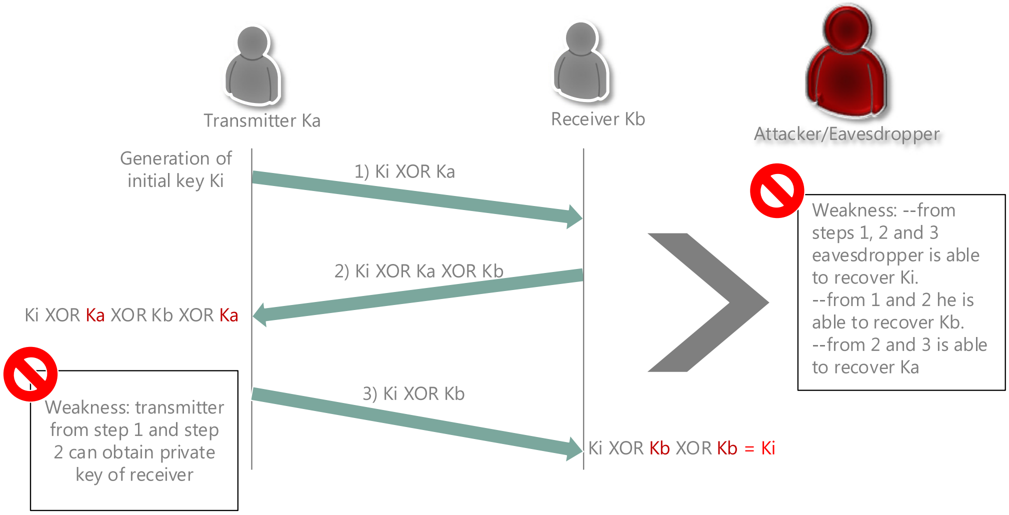

Transmitter Ka
Receiver Kb
Attacker/Eavesdropper
Generation of initial key Ki
1) Ki XOR Ka
2) Ki XOR Ka XOR Kb
Ki XOR Ka XOR Kb XOR Ka
3) Ki XOR Kb
Ki XOR Kb XOR Kb = Ki
Weakness: transmitter from step 1 and step 2 can obtain private key of receiver
Weakness: --from steps 1, 2 and 3 eavesdropper is able to recover Ki.
--from 1 and 2 he is able to recover Kb.
--from 2 and 3 is able to recover Ka

Fig. 19. Key distribution method based on XOR operation [103].

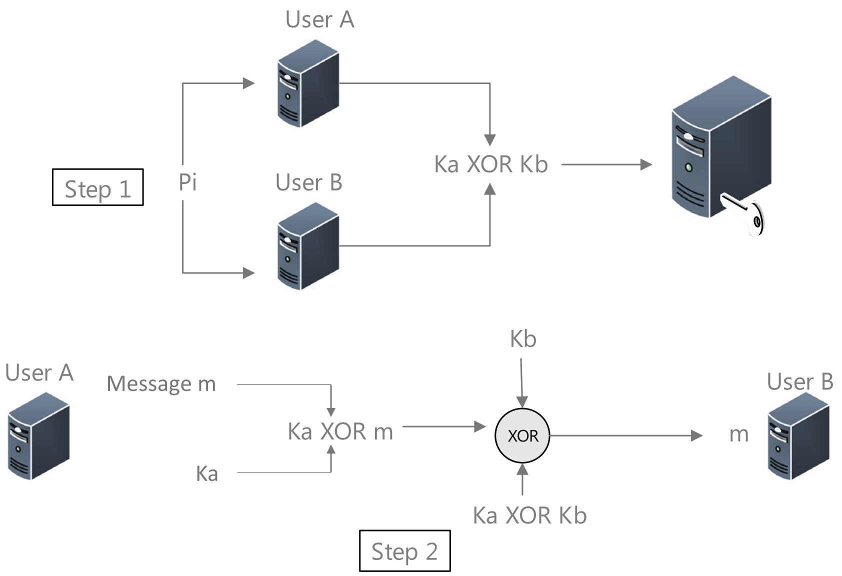


Fig. 20. A schematic of the secret key generation technique presented in [104].

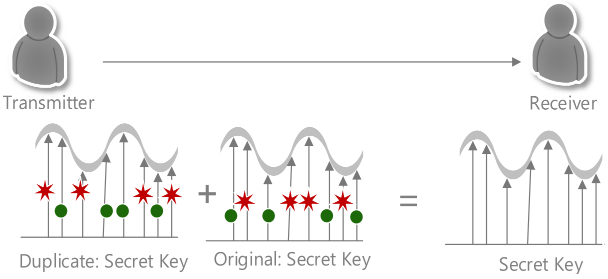


Fig. 21. A keyless key distribution method based on jamming in [109].

Whereas in [17], encryption keys are obtained from the bipolar real OFDM samples (the cyclic prefix) at the output of the optical OFDM systems. This technique is considered weak since encryption keys should never depend on the transmitted payload due to fading and channel noise.

In [109], the authors present a novel technique, iJam (Fig. 21), that uses "cooperative jamming" for key distribution among users. The intuition behind this technique is that there is no need for any pre-shared information between the transmitter and receiver. In the iJam technique, the transmitter sends two copies of each OFDM symbol back-to-back. The receiver, which is in this case also the jammer, randomly jams complimentary samples in the original signal and its repetition. Upon reception, the receiver picks out the correct samples from the signal and its repetition and re-arranges them to get the intended signal since only the jammer knows which samples are clean and which are jammed. The eavesdropper, on the other hand, cannot differentiate between the clean and jammed samples, thus, is not able to detect the data correctly. In this technique two OFDM symbols are sent back-to-back, which is unpractical. In principle, each symbol should be acknowledged separately and there should exist a time slot between symbols.

A general overview of PLS for the Internet of Things (IoT) is presented in [110]. More specifically, the authors highlight the secret key generation issue and present one technique that enables two entities to exchange the secret session key securely. User A sends a public pilot signal to user B, which will enable B to estimate the CSI. Again user B, after a certain time τ, sends a pilot, which enables A to estimate the corresponding CSI. These steps are repeated several times until both users get enough measurements to generate a set of keys. Since the measurements of both users might not be equal, users can exchange and compare the time stamps of the measurements. These time stamps might not be equal, however, their difference should be equal to the sampling delay in TDD mode. In turn, both users will exchange their time stamps and each will keep the common ones only. As such, both have the paired measurements and thus, are able to extract the secret key used for encryption.

Non-reciprocity is also addressed in [111]. A novel channel gain complement (CGC) algorithm is presented. This scheme can mitigate the CSI disparity between a pair of wireless devices by removing the non-reciprocity component, which is obtained from a small number of probe packets only: After collecting a certain number of samples of CSI, each of the two users send the extracted CSI samples together with the corresponding time stamps to the other user. Then, the time stamps of both users are compared. Only the samples with time stamps on both sides satisfying the following requirement are utilized for non-reciprocity learning: the difference between the time stamps should be less than the threshold of the coherence time. Here, it should be noted that time stamps can also be retrieved by an eavesdropper making the presented technique not completely secure against attackers.

In [113], a robust key generation technique is presented and it is mainly divided into two steps. In the first step, users estimate their channel gains which are considered primary random processes and compare them to a preset threshold. If the channel gain exceeds the threshold, the location is stored in a vector S (initially all zeros). From the primary random process, a secondary random process is derived which is in turn used to generate the secret keys. The primary random process is compared to a preset threshold. After setting vector S, the moving increments, which are the difference between each two adjacent locations, serve as the realizations of the second random process. Finally, both users generate the secret key from the secondary random process. Again, in this technique, key generation mainly depends on the channel between the users and thus suffers from the previously mentioned drawbacks.

Table 3
A summary of the common sources of randomness.

Common source of randomness	Channel estimates	RSS	Distance	AoA
Advantage	No additional cost and overhead	No additional overhead in terms of resources and latency	Simple and good for mobile scenarios	High estimation accuracy at low SNR levels
Limitation	AWGN affects the reciprocity of the channel	A mobile scenario is needed	Vulnerable to being recovered if receiver has AoA capabilities and user should be mobile	Additional hardware and computationally complex

In [112], the authors use a different approach to establish session keys between legitimate users relying on keyless cryptography (Fig. 22). The presented protocol consists of:

- **Initialization**: A public trusted authority generates the training sequence.
- **Training**: Legitimate users move into proximity (move their devices close to each other) and exchange the training sequences, which in principle will have different shifts in amplitude, phase, and frequency. After receiving the training sequences, the corresponding mismatch is evaluated.
- **Signal Transmission**: Users exchange several rounds of random analog signals to mask the mismatch in such a way that if the first signal in a specific round belongs to user A, the corresponding bit is set to "1", otherwise it is set to "0". At each round, a secret bit of the key is obtained.
- **Key Establishment**: In this step, the secret key is generated.

In [97], the authors introduce three metrics that are essential for the evaluation of key generation systems: (1) Randomness, which is the most important feature in key generation and it is tested using the randomness tests provided by the National Institute of Standards and Technology (NIST), (2) Key Generation Rate (KGR), which is the amount of secret bits generated in one second, and (3) Key Disagreement Rate (KDR), which is the percentage of different bits in the generated keys of two communicating users. The different aspects and fundamentals of secret key generation in PLS are discussed in the survey of [114]. First, the authors discuss the common sources of randomness, which are shown in Fig. 23, summarized in Table 3, and described below:

- **Channel estimates**: The most popular randomness metric used in PLS is the channel gain and the channel phase, which fall under this category. These metrics can be easily estimated and result in high key generation rate. However, one drawback of using channel gain or channel phase in key generation

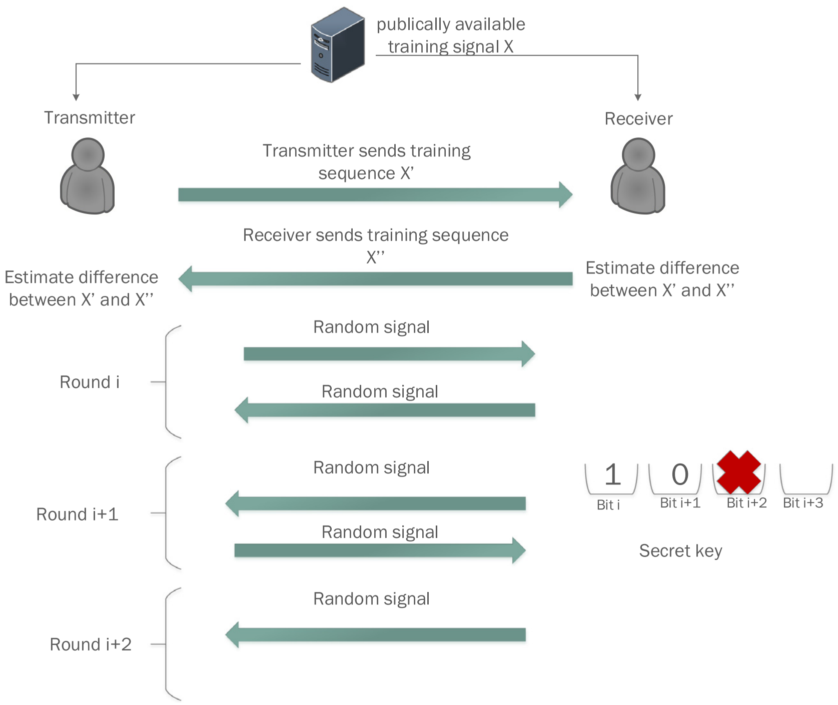

publically available training signal X
Transmitter
Receiver
Transmitter sends training sequence X'
Receiver sends training sequence X''
Estimate difference between X' and X''
Estimate difference between X' and X''
Round i
Random signal
Random signal
Round i+1
Random signal
Random signal
Round i+2
Random signal
1
0
Bit i
Bit i+1
Bit i+2
Bit i+3
Secret key

Fig. 22. Secret key generation technique using keyless cryptography in [112].

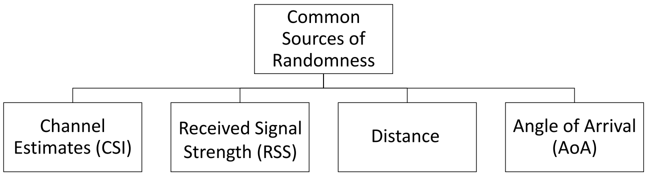


Fig. 23. Common sources of randomness in wireless channels at the physical layer [114].

is the additive white Gaussian noise (AWGN), which affects the reciprocity of the channel between two users.

- **Received signal strength (RSS) indicator**: The RSS is the received signal's power. This common metric can be implemented easily; however, in order to generate a key with acceptable entropy/randomness, a highly mobile scenario should be considered, which is not a practical assumption.
- **Distance**: Similar to the RSS indicator, this metric is best suited for mobile scenarios. However, a major weakness is that a generated key based on distance is vulnerable to being recovered if an eavesdropper is equipped with angle of arrival (AoA) estimation capabilities.
- **Angle of Arrival (AoA)**: One advantage of using AoA as a common source of randomness in secret key generation is its high estimation accuracy at low SNR levels [114]. However, it requires additional hardware and is more computationally complex.

Afterwards, the authors present and discuss the steps for key generation (Fig. 24):

1. **Initialization**: In this step, users exchange beacons or dummy data
2. **Common source of randomness estimation**: Legitimate users estimate the physical layer channel characteristic based on the received signal from the other legitimate node.

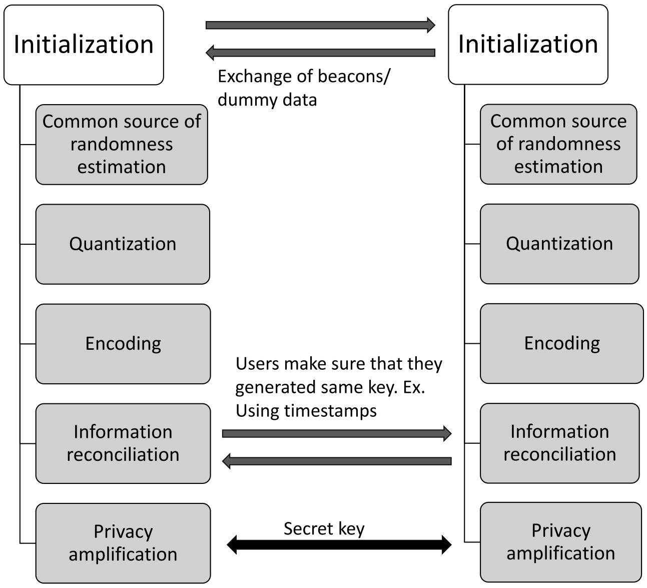

Initialization
Initialization
Exchange of beacons/ dummy data
Common source of randomness estimation
Common source of randomness estimation
Quantization
Quantization
Encoding
Encoding
Users make sure that they generated same key. Ex. Using timestamps
Information reconciliation
Information reconciliation
Secret key
Privacy amplification
Privacy amplification

Fig. 24. Key generation steps as presented in [114].

3. **Quantization**: The users convert the estimated common source of randomness to bits. This topic is discussed thoroughly in [115].
4. **Encoding**: To avoid mismatch in bit rate between two users, each quantized value is encoded.
5. **Information reconciliation**: This step is crucial since there may exist some differences in the generated bit streams between two users due to interference, noise and hardware limitations, which leads to inconsistency in the generated secret key. In this step, users make sure that the keys generated at both ends are the same.
6. **Privacy amplification**: This step is directly linked to the previous one since information reconciliation leaks some

information, which will in turn be useful to an eavesdropper to recover the secret key. To avoid this issue, privacy amplification reduces the length of the output bits and prevents the leakage of any information related to the agreed key. This can be realized through a set of hashing functions [97,114].

Three of the above steps are evaluated and simulated in [116]: the distillation phase (Common source of randomness estimation), the reconciliation phase and the privacy amplification phase using Matlab.

Finally, the authors in [114] divide the commonly used metrics in secret key evaluation into information theoretic metrics and statistical metrics. Information theoretic metrics include: secret key rate, secret key capacity and outage secret key capacity. Statistical metrics include: frequency test, serial test, poker test, run test, auto-correlation test and bit mismatch rate.

However, a more accurate categorization of metric evaluation is shown in Fig. 25. Typically, metrics evaluation is based on two important factors, the efficiency of a specific security algorithm and its security level. Efficiency includes the secret rate, latency and required resources, while security level includes resistance against attacks, independence and uniformity. The last two metrics are evaluated using randomness statistical tests. Unlike [114], Fig. 25 is more general.

In [117], the authors analyze and evaluate the secret key and privacy leakage rate of a binary secret key scheme, called fuzzy commitment. This scheme is different since a transmitter encrypts the secret key and then XORs it with the transmitted message. The result is referred to as the public data helper, M, and it is sent to the receiver through an authenticated and noiseless channel. The transmitter then sends the message through the noisy channel. The received signal is then XORed with M and the secret key is thus estimated. However, the assumption of having an authenticated link between two legitimate users is not a practical one.

The technique in [118], on the other hand, relies on a third party authority for session key distribution. This technique cannot be generalized since in some cases we do not have a trusted public authority where end-to-end key generation and distribution protocols are more desirable.

In [119] a key extraction protocol for D2D communication is presented and is studied experimentally. It has been shown that adjacent or nearby sub-carriers have similar physical characteristics, thus their corresponding CSI measurements may have strong correlations, which is a major vulnerability that should be addressed. For this purpose, the authors presented a fast secret key extraction protocol, KEEP, which combines the information of all sub-carriers. This validation-recombination mechanism prevents attackers from obtaining the secret keys, thus, achieving high security level and fast key-generation rate.

All of the schemes presented so far mainly depend on the channel and more specifically assume that the channel responses of both the sender and receiver are identical, which might not be the case all the time. The authors of [120] study experimentally the non-reciprocity factors of CSI from the perspective of hardware devices mismatches and time delay. The evaluation is done using the Mean Square Error (MSE) algorithm.

In [11], the authors verify the feasibility of a key generation technique through implementation on the wireless open-access research platform (WARP) [121] running an 802.11 OFDM system. The investigated scheme simply generates secret keys from the channel responses of individual sub-carriers in OFDM systems.

Unlike the techniques that preceded, [122] and [10] analyze the security of the shared session keys between users rather than introducing new key generation and distribution techniques. In [10], the authors mainly consider sophisticated attacks that enable an attacker to manipulate the key generation process and go unnoticed. More specifically, the following two types of attacks are considered: (1) different-key attacks and (2) low-rate key attacks. The former attack is when an insider tries to force different realizations of the shared secret key at different nodes. The latter is when an insider tries to reduce the secret-key rate by decreasing the channel variations over time. Whereas in [122] the authors prove, through information-theoretic analysis, that the secret key capacity of the side-channel is lower than that of the wiretap channel. In addition, the authors analyze the electronic devices during randomness capturing and quantization and consequently show that the keys generated from the physical layer are susceptible to many threats.

The above mentioned key generation and distribution techniques can be summarized into five groups, shown in Fig. 26.

6. Data confidentiality techniques

In this section, different schemes that target data confidentiality are summarized and compared in Fig. 27 and Table 4.

6.1. Data confidentiality schemes

Fig. 28 illustrates the existing OFDM cipher schemes that are described in more detail in this part of the survey. Encryption in OFDM-based systems is divided into two main classes: Pre-OFDM encryption and Post-OFDM encryption. In the former class, frequency-domain symbols are encrypted (before passing through the IFFT block), While in the latter, time-domain symbols are encrypted (after the IFFT block). In this subsection, data confidentiality schemes are first listed and described. Then, a comparative study based on simulation tests is presented to evaluate the performance of the two classes of encryption schemes, followed by some conclusions.

6.1.1. Permutation

One simple approach to secure transmitted data is through permutation and interleaving. In [21], the “Cyclic Delay Perturbation on Effective Channel (CDPEC)” scheme is presented for the MISO (multiple-input single-output) single-antenna-eavesdropper wiretap channel. The scheme improves PLS in OFDM systems through introducing a random cyclic delay (perturbation) to the transmitted signals. The random perturbation, which changes per symbol, depends on the CSI between the legitimate users and the total transmit power, both of which are available at the intended transmitter and receiver only. Basically, before appending the cyclic prefix (CP), the time-domain signal resulting from the IFFT block on a specific antenna, is cyclically shifted by a specific delay. As a result, the effective channels experienced by both the intended receiver and the eavesdropper are changed into linear combinations of phase-rotated channel gains. At the receiver’s side, the cyclically shifted signal is multiplied by a weighting factor in the frequency domain, such that only the intended receiver is able to generate this factor and recover the real signal. For this scheme, no additional information about the eavesdropper’s channel is required at the transmitter side and no additional information with the transmitter is necessary at the receiver side.

Another technique for enhancing PLS is through signal interleaving, in which the time and/or frequency domain signals are shuffled based on chaotic pseudo-random sequences [22]. In [40] and [28], interleaving is done before and after the IFFT block based on a key stream (pseudo-random sequence) generated by a chaotic map, which results in a two-level data encryption since both the time and frequency domain signals are interleaved. The method is similar to the one presented in [27], except for the fact that securing the OFDM system is achieved using time domain scrambling only, which is based on a pre-shared secret key. On the other hand, chaotic-based encryption solutions have proven to

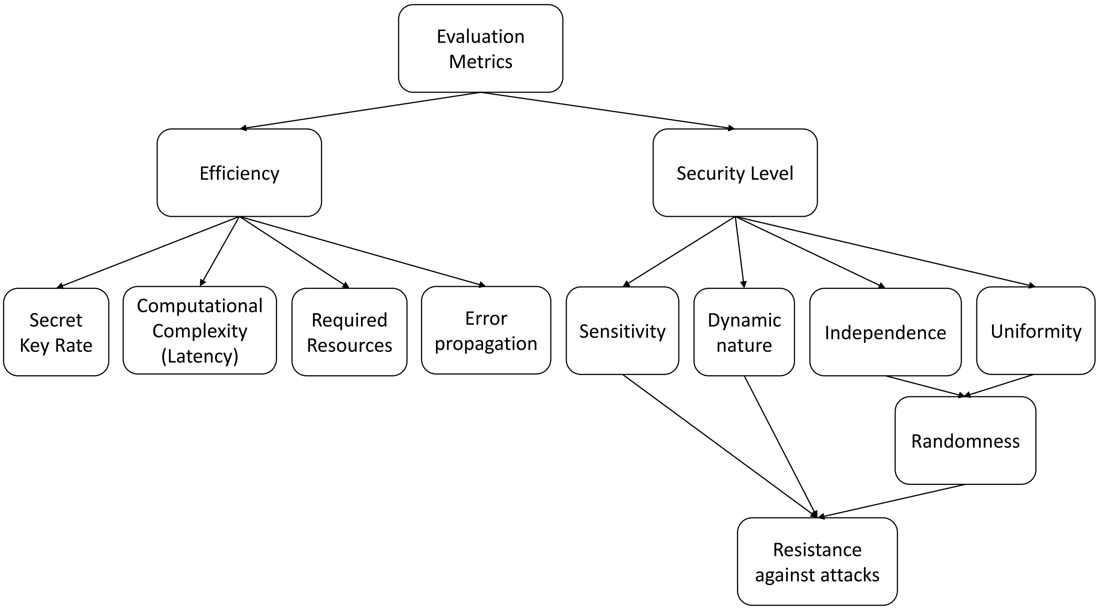


Fig. 25. Chosen metrics used for the evaluation of key generation and encryption techniques.

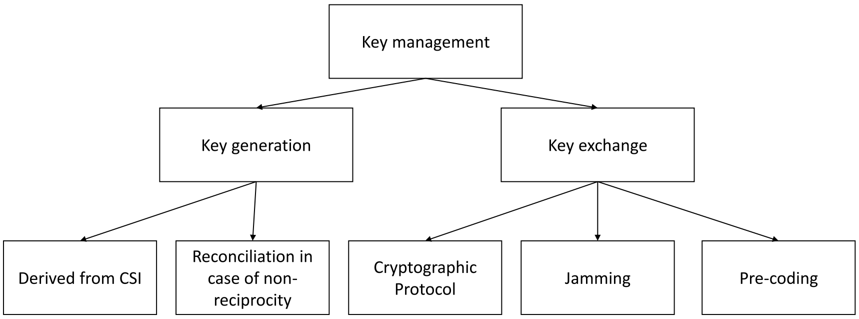


Fig. 26. Existing key generation and distribution methods. Some methods achieve key generation and distribution at the same time.

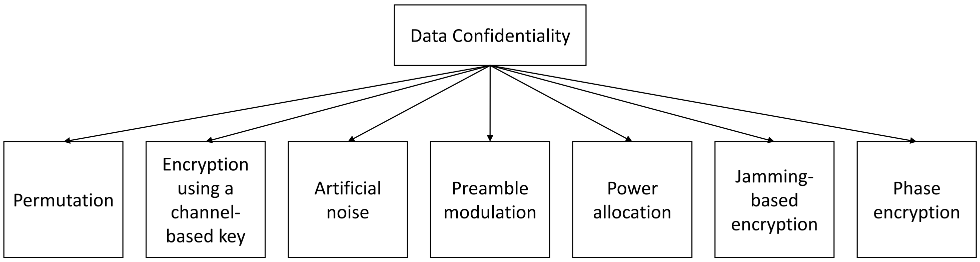


Fig. 27. Proposed data confidentially technique classification for OFDM systems.

be inefficient and not fully secure due to their poor cryptographic structure, in addition to having several disadvantages such as high computational complexity, memory and energy consumption.

In contrast, a new technique that provides practical secrecy is presented in [23]; OFDM sub-channels are shuffled based on the intended user's channel. The transmitter extracts the unitary matrices from the amplitude of the channel frequency diagonal matrix of the legitimate user. The resulting unitary matrices are then decomposed using singular value decomposition (SVD) and used as channel frequency-based precoder and post-coder. In this method, the authors rely on the channel randomness for achieving OFDM system security.

Moreover, random permutation can also be realized when the real and imaginary components of a symbol are interleaved, as is the case in [38]. Specifically, this is done when the channel phase of a sub-carrier symbol is larger than a predefined threshold.

The main advantages of the techniques presented in this subsection are simplicity, low computational complexity and low energy. However, these techniques lack the notion of secrecy, in which data shuffling is done based on known parameters that can be acquired easily.

6.1.2. *Phase encryption*

In [123], a PLS encryption scheme based on pseudo-random phase permutation is presented at the time-domain signal level. Two pseudo-random sequences *a* and *b* are generated using secure stream ciphering, where sequence *a* is multiplied by the real part of the time domain signal, and sequence *b* is multiplied by the imaginary part. This represents pseudo-random phase shuffling of

Table 4
A summary of the OFDM data confidentiality schemes presented in the literature.

Data confidentiality for OFDM systems	Permutation	Phase encryption	Artificial noise (AN) and artificial fast fading (AFF)	Channel state information (CSI)	Jamming	Encryption / PAPR reduction
Advantage	Low computational complexity and low energy	Simplicity and low cost	Automatic cancellation of AN and AFF when passing through the intended channel. No further actions done at the receiver	Ciphertext is resilient to cryptanalysis	Data hiding	Joint PAPR reduction and enhanced security levels
Limitation	Weak level of security since it is based on channel properties only	Vulnerable to brute force attack since there are only four possible combinations that can be used for encryption	Eavesdropper can recover transmitted data if it is aligned with the legitimate receiver	CSI can be easily obtained if the eavesdropper is synchronized with the legitimate users	Data distortion and eavesdropper should not be aligned with legitimate users Overhead increase in terms of communication and latency and data rate reduction	Large delays and computational complexity. Also the receiver has to detect the sequence used for the transmitted sequence
Resource and communication cost	No additional cost and overhead	Generation of two pseudo-random sequences	Generation of AN and AFF matrices from the decomposition of the channel matrix	No additional resource and communication cost	Additional resources are needed to send jamming signals (more power)	Generation of several sequences
Complexity	Not computationally complex: performing shuffling and permutation	(1) Divide each complex symbol into real and imaginary, (2) multiply the real and imaginary with the generated sequences and then (3) form again the complex symbol	(1) Extract information from channel. (2) Generate AN and AFF. (3) Include these signals in transmitted data	Data multiplication with extracted channel information	Generate and send jamming signals	(1) Generate several sequences, (2) choose one with the lowest PAPR
Recommendation	Integrating a secret in the construction of scrambling matrix	Integrate a secret or perform a two-level encryption	Preamble encryption and/or deriving a dynamic secret key using the original secret key and the AN/AFF	Preamble encryption to prevent eavesdropper synchronization with legitimate users, hence obtaining the CSI and integrating a secret with the extracted CSI	Encrypt transmitted data since eavesdropper might be aligned with users Dynamic subcarrier allocation based on a secret and CSI	Perform time-domain encryption (Pre-IFFT)

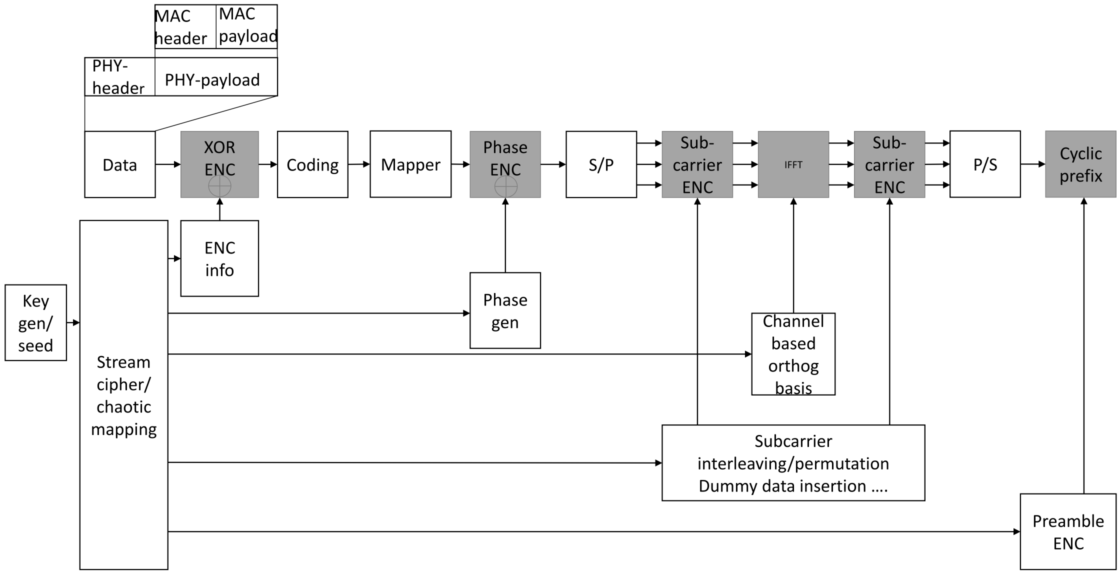


Fig. 28. Existing OFDM PLS encryption schemes.

the in-phase and quadrature symbol components. The sequences a and b can be either ±1, and thus, each symbol has only four possible combinations, making this scheme vulnerable to brute force or dictionary attacks, especially if a static secret key is used.

6.1.3. Channel-based data encryption

Towards securing the physical layer, most researchers rely on the channel properties to build a secret key, which is considered one of the main innovations in this area.

One way of doing so is through active sub-carrier index selection. In the index selection scheme of [36], the data bits are divided into two groups. The first group of bits represents the indices of the active sub-carriers that will be used to carry the second group of data bits, which are part of the real data. The selection of active sub-carriers depends on the CSI between the transmitter and receiver, and which are arranged in descending order of their channel gains observed at the transmitter. Here, an eavesdropper receives incorrect symbols due to the unknown CSI used for index selection and data modulation. However, this is not always true since in case the eavesdropper is able to synchronize to the transmitted data, the CSI can be estimated easily. The authors of [37], also use sub-carrier index selection for securing physical layer data. The difference here is that only the sub-carriers experiencing high channel gains are used to transmit data. The main motivation behind this scheme is that while the channel gains of some sub-carriers are high between two users, these sub-carriers might experience low channel gains for other sets of users, which affects the data rate dramatically.

A novel OFDM physical layer encryption scheme using dummy data insertion is presented in [5] and [25]. The main idea is to obfuscate the encrypted data streams by randomly inserting dummy data at random OFDM sub-carriers using $[s, k]$, where s is the number of OFDM symbols per data unit and k is the number of dummy data per data unit. As such, the encrypted data will be secured and only legitimate users will be able to (1) know the locations of the dummy data and (2) remove them in order to decrypt the sent signals and in turn (3) recover the real data at the intended receiver side. In [5], the location of dummy data differs between OFDM symbols. These locations depend on a secret shared "seed" between legitimate users. Thus, the seed serves two purposes; first, it is used for generating a stream cipher that represents the sub-carrier location of dummy data and second, it is used to generate another stream cipher, which represents the dummy data itself, as shown in Fig. 29. At the receiver side, data can be recovered since only the legitimate users share the encryption information. In this technique, the data rate is inversely proportional to the security level; the security of the presented scheme improves with the increased number of dummy data, which leads to reduced data rates. The authors also introduced an added security feature, training sequence re-arranging, which prevents an eavesdropper from performing synchronization and channel estimation correctly since she has no access to the new training sequence, which is only shared between the transmitter and receiver.

The authors of [25] design secure pilot signals (SPSs) to help the legitimate receiver differentiate between real and dummy data and thus, recover them. In particular, SPSs are designed in such a way that only the intended user is able to locate the sub-carriers carrying real data. In the two previous methods, the eavesdropper has to guess the location of the real data and extract them from the received signal. This is only true when the eavesdropper has absolutely no knowledge about the channel between the legitimate users.

In [9], the authors present a novel scheme in which the traditional fixed IFFT/FFT blocks are replaced with new ones. The new blocks are based on the channel (H) between the legitimate transmitter and receiver and are used to perform the modulation function in a secure manner. Basically, new orthogonal bases are extracted from the channel, decomposed into new matrices (SVD) and then are used to transmit and receive data. As such, only the legitimate receiver is capable of retrieving the sent data since it is able to estimate the channel and derive the basis used for transmission.

Notations: vectors are denoted by bold-small letters, whereas matrices are denoted by bold-large letters. I is an identity matrix. The transpose, hermitian (conjugate transpose) and inverse are symbolized by $(\cdot)^T$, $(\cdot)^H$ and $(\cdot)^{-1}$, respectively.

The detailed description of the presented technique is shown in Fig. 30 and works as follows: First, H, which is extracted from the legitimate user's channel, is decomposed using singular value decomposition (SVD):

$$\mathbf{H} = \mathbf{U} \cdot \mathbf{E} \cdot \mathbf{V^H} \tag{3}$$

Then, the transmitter multiplies the transmitted symbols **s** with **V**, which results in: $\mathbf{x} = \mathbf{Vs}$. Neglecting the AWGN, the obtained signal at the receiver's side is: $\mathbf{y} = \mathbf{Hx}$. In order to obtain **s**, the receiver performs equalization and multiplies by $\mathbf{U^H}$, resulting in:

$$\mathbf{E^{-1}} \cdot \mathbf{U^H} \cdot \mathbf{y} = \mathbf{E^{-1}} \cdot \mathbf{U^H} \cdot (\mathbf{U} \cdot \mathbf{E} \cdot \mathbf{V^H} \cdot \mathbf{V} \cdot \mathbf{s}) = \mathbf{s} \tag{4}$$

where $U^H \cdot U = I$ and $E^{-1} \cdot E = I$. Here, the multiplication of **s** with V and U^H at the transmitter and receiver, respectively, will be canceled out when passing through the intended channel (H), hence securing the data transmitted, which will only be recovered by the intended receiver.

Any eavesdropper, on the other hand, will not be able to recover the real data unless she is able to correctly estimate the channel, which is not a practical assumption. In addition, this scheme requires matrix multiplication which introduces considerable overhead in terms of resources and latency, in comparison to the permutation scheme.

Similarly, the transmitter in [35] estimates the channel between itself and the intended receiver and then, modifies the transmitted signal according to the CSI using pre-equalization. At the receiver, the pre-equalized signal will change to an undistorted signal only when passing through the intended channel.

The data encryption scheme presented in [34] works as follows: legitimate users estimate the CSI between them, share transform orders and modulate data accordingly. In this scheme, only users with valid transform orders are able to demodulate the data.

On the other hand, the authors of [41] exploit the fact that the imaginary part of transmitted symbols is usually unloaded to introduce a new physical layer encryption (PLE) method for OFDM/OQAM based on intrinsic interference. Consequently, the imaginary part of the symbol can be used as an encryption key to obfuscate the sent data symbols. For eavesdroppers, it is very difficult to recover the data since a secret key is required. In contrast, legitimate receivers are able to recover the sent data by eliminating the interference completely.

Differently, the authors of [20] introduce the idea of each sub-carrier having a distinct initial phase. In particular, a new mechanism to achieve angle-range-dependent physical layer security for point-to-point communications is presented in which the transmitted OFDM symbols are well preserved in a specific location, while symbols are scrambled at all other locations. The algorithm produces a unique phase for each sub-carrier of the OFDM symbol in baseband. Here, a (MISO) system is considered. In traditional beamforming, each element is equipped with a phase shifter and each symbol is weighted with a specific weight to target a desired transmission direction [20]. At the receiver side, the modulated OFDM symbols are recovered correctly along a specific direction but not elsewhere. However, this method cannot guarantee good security when an eavesdropper is equipped with a sufficiently sensitive receiver. For this reason, the authors resort to an enhanced and more secure technique than conventional beamforming.

Additionally, two types of encryption techniques are also present in the literature, XOR encryption and phase encryption. In [24], these techniques are compared in terms of decoding symbol rate, where the first technique is conventional encryption: stream cipher encryption using XOR and the second is achieved by

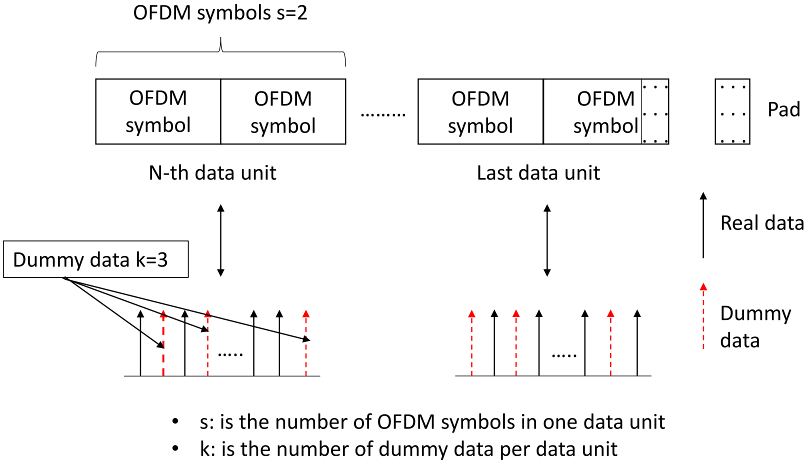


Fig. 29. Encrypting data using dummy data insertion with [s,k] = [2,3] [5].

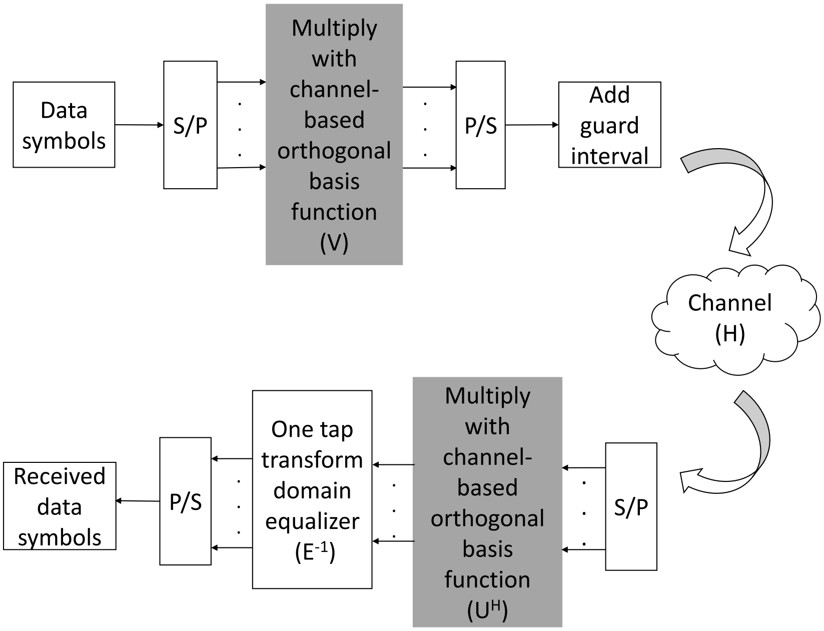

Data symbols
S/P
Multiply with channel-based orthogonal basis function (V)
P/S
Add guard interval
Channel (H)
S/P
Multiply with channel-based orthogonal basis function (U^H)
One tap transform domain equalizer (E^-1)
P/S
Received data symbols

Fig. 30. The data encryption technique in [9], which presents a new IFFT/FFT blocks derived from the channel.

multiplying the real and imaginary components of the time domain OFDM samples by two binary key streams $\{1, -1\}$.

The chaos I/Q-encryption technique presented in [3] is also a step forward towards a more secure physical layer; after serial to parallel (S/P) conversion and QAM mapping, QAM symbols are split into two parts: In-phase (I) and Quadrature-phase (Q). Each part is then multiplied separately by a phase sequence which is generated using a chaotic map. The technique presented in [26] is also based on a chaotic system, which generates 3-D chaotic sequences. However, in this scheme the generated sequences are used to form the training sequences of the OFDM frames, OFDM sub-carrier masking and control the fractional order of the FFT operation. Similarly, this approach suffers from the previously mentioned chaotic PLS limitations and challenges.

Another technique that utilizes chaotic mapping is presented in [18]. Here, the authors apply logistic chaotic maps to enhance the security of OFDM systems in VLC. More specifically, the proposed scheme exploits the random nature of the physical channel, mainly CSI, and the symbol's Cyclic Prefix (CP) to:

1. Permute frequency-domain symbols using column/row permutation,
2. Encrypt time-domain signals using a secret key.

Typically, a chaotic system introduces a significant overhead in terms of latency and resources requirement since it is based on floating-point arithmetic. Moreover, the secret key depends on the symbol CP, which copies the last bits of the previous symbol and multiplies them with the channel-based chaotic sequences to encrypt the current symbol. This is considered a major weakness since a secret key should be independent of plaintext/ciphertext. In fact, the secret key should never depend on the transmitted payload (or CP) and consequently should not depend on the CP due to interference and transmission errors.

In contrast, authors in [124] exploit both, channel characteristics and the OFDM symbol structure (CP) to enhance the security of OFDM systems using the channel shortening (CS) method. More specifically, they propose using a smaller CP and applying CS at the transmitter's side, in such a way that the effective channel at the receiver's side does not cause ISI, while effective channel of the eavesdropper causes ISI.

What is common to all the techniques presented in this subsection is that the CSI is utilized as a secret key between two legitimate users for encryption (confidentiality). The main motivation behind this approach is that the channel between any two users is unique, dynamic, always varying and pseudo-random. Hence, the channel characteristics can be used in the encryption process, more specifically in the secret-key generation. However, the above techniques suffer from a major drawback since they all rely on the estimated CSI solely assuming that the eavesdropper is unable to estimate the CSI between any two legitimate users. In reality, the eavesdropper can get the CSI if she is able to synchronize to the transmitted data, which is achieved through preamble detection and synchronization.

6.1.4. Artificial noise and artificial fast fading

The technique presented in [19] requires the cooperation of both the sender and receiver, and the addition of artificial noise (AN) to the transmitted time-domain signal. Also, an OFDM single-antenna relay system is considered. Unlike most existing AN techniques, which only consider MIMO systems, the authors consider a system where all users are equipped with a single antenna. The mechanism is summarized as follows: the sender and receiver estimate the channel and obtain the CSI. Using the IFFT block, the sender transforms the frequency domain signal to time-domain, appends the CP at the beginning of each OFDM symbol, adds the AN, which is derived from the estimated CSI, and transmits the signal to the relay. Then, the receiver sends a jamming signal to the relay, which is regarded as self-interference and cancels the AN. Consequently, the eavesdropper receives the distorted signal and is unable to recover it.

In [39], the authors use the carrier frequency offset (CFO) as a new feature to incorporate AN in a physical layer security scheme. In principle, CFO is the difference between the frequencies generated by the transmitter's local oscillator and the local oscillator within the receiver. The basic idea is to pre-compensate the carrier frequency offset in the transmitted data in such a way that when it passes through the legitimate receiver's channel, the signal will be received without ICI.

Additionally, artificial fast fading (AFF) is exploited in [4] to improve the energy efficiency of MISO systems using OFDM. On the other hand, using AFF also adds to physical layer security in such a way that the pre-introduced weights at the transmitter side, and which are derived from CSI of the channel shared between two users, will be canceled out when propagating through the intended channel. Thus, only the intended receiver will be able to recover the real data easily.

As it can also be inferred here, the mentioned schemes use CSI to pre-equalize or pre-compensate the transmitted signal such that this added noise would cancel out when passing through a legitimate user's channel. Considering that the eavesdropper is able to access the related information, the performance of these technique would suffer greatly.

6.1.5. Preamble encryption

In order to prevent an eavesdropper from estimating the channel between two users and extracting the CSI through signal synchronization, preamble security should be enhanced.

Generally, especially in OFDM-based systems (802.11), the receiver does not know the exact signal of the preamble but knows its structure. This has motivated the authors of [15] to construct several new, but compliant preamble waveforms. To generate such waveforms, a new technique, called preamble modulation (P-modulation), is presented. P-modulation is a combination of two signal processing techniques, namely shift in time-domain and phase rotation in frequency domain. Differently, the mechanism presented in [16] manipulates the preamble sequence based on the CSI shared between two users. In addition, two power efficient algorithms are introduced enabling the intended receiver to correctly estimate the channel.

Moreover, another way to improve preamble security is through embedding user-specific data not known to the eavesdropper or sequence permutation. In [5], as mentioned earlier, the long training sequence is re-arranged in a manner only known to the legitimate users, which will prevent CSI and CFO estimation at the attacker side.

Securing the packet preamble is necessary to prevent eavesdroppers from synchronizing with legitimate users and acquiring the channel state information. However, this is only one layer of security that should complement data confidentiality schemes.

6.1.6. Power allocation

A technique referred to as "frequency diverse array (FDA) beamforming" is presented in [29] and [30]. The main idea is to maximize the secrecy rate by carefully designing the following parameters: frequency offsets across the antennas and the transmit beamformer. First, the channels of both the legitimate user and the eavesdropper should be maximally decoupled by optimizing the frequency offsets across the array elements. Essentially, the frequency offset values affect the phase lags among different array elements, which leads to independent channel characteristics among different users. Given the set of frequency offsets, the transmit beamformer can thus be optimized.

The commonly used PLS schemes such as beamforming and AN-insertion fail in certain environments due to the high correlation between the eavesdropper' channel and the intended users such as the case in Line-of-Sight (LOS) mmWave communications. To solve this issue, several techniques related to power allocation for securing communication are presented in the literature [125,126].

One of the main features in OFDM-based networks is the fact that each sub-carrier experiences different gains values. In [32], a two-step PLS scheme is presented and it includes optimal power distribution and multi-user sub-carrier allocation. Initially, the transmitter estimates and then allocates the optimal transmit power for each sub-carrier. Afterwards, two algorithms are introduced to effectively allocate sub-carriers among several users. Accordingly, both the secrecy rate and the performance in terms of fairness among users are greatly improved.

In [127], the authors jointly optimize subcarrier power allocation and the covariance matrix of the time-domain artificial noise to improve the secrecy rate (nonconcave function).

The resource allocation problem to achieve PLS in heterogeneous networks is also addressed in [33]. The main idea is similar to the one presented above: finding transmit power vector (also referred to as sub-carrier allocation vector), which is modeled as an optimization problem. In other words, the main target is to find the optimal power for each sub-carrier, in addition to finding the optimal set of active sub-carriers.

A similar concept to power allocation is optimal resource allocation for secure communication networks. The work presented in [128–130] is based on the fact that the security in a multi-user OFDMA-based system can be significantly improved by well-designed resource allocation schemes, which enhances greatly the secrecy rate of users.

On another note, the basic idea behind the approach presented in [31] is that the cooperative jammer uses the harvest-then-jam protocol to ensure the protection of confidential information in transmission. The transmission block is divided into two time slots. In the first slot, the source sends dedicated energy signals to the receiver, which acts as the jammer. In the second slot, the jammer uses the harvested energy to interfere with the eavesdropper.

Again, a secret key is needed to ensure a good level of PLS.

6.1.7. Jamming-based encryption

In order to avoid the challenge of key generation and distribution between users to ensure data confidentiality, the authors in [42] design and implement a keyless acoustic short-range communication system, PriWhisper, which exploits friendly jamming technique from radio communication. The system allows the receiver to send a random jamming signal while the transmitter is transmitting, and since the receiver knows the jamming signal it is emitting it can simply remove the noise and receive the intended data.

However, jamming cancellation can be a very exhaustive and computationally complex task, which can be done either by generating an antidote signal or estimating the jamming signal from the received signal. Both techniques require a lot of resources and thus, are not feasible for implementation.

6.1.8. Joint PLS enhancement and PAPR reduction

A major disadvantage in OFDM systems is having the overall instantaneous power greater than the average power, leading to high PAPR, which results from high time-domain peaks that are produced when independently modulated sub-carriers are coherently added. Therefore, several works in the literature have been presented to jointly reduce PAPR values and enhance PLS such as [3] and [131]. These techniques have already been discussed in earlier subsections. It should be noted that PAPR reduction is an important issue in OFDM systems but is not the focus of this survey and hence, it will not be further discussed.

6.2. Channel and hardware impairments

Channel and hardware impairments, which occur frequently during communication, hinder the efficient deployment of PLS techniques and jeopardize the security of transmitted data. On the other hand, several schemes have emerged recently, and which exploit this weakness to achieve strong secrecy.

- **Synchronization errors**: In principle, synchronization errors prevent users from performing time/frequency synchronization. This causes a significant degradation in performance since one cannot compensate for the effects of Carrier Frequency Offset (CFO) and/or Symbol Time Offset (STO) [132]. The presented scheme in [133] intentionally suppresses the cyclo-stationary feature of the cyclic prefix, which causes synchronization errors at the illegitimate user and prevents her from detecting this feature.
- **Non-linear conversion operation**: Here, the non-linearity of the power amplifier can be used to enhance the security of transmitted data such as the case in [134]. More specifically, the transmitter can pre-compensate data such that it has large fluctuations at the input of the adversary's power amplifier, and smooth steady magnitude at the legitimate receiver's side [132].
- **IQ imbalance and phase noise**: Based on [135] and [136], it has been shown that IQ imbalance and phase noise should be taken into consideration when designing secure wireless systems since both negatively affect the security level and performance. Consequently, this can be exploited in such a way that only legitimate users are able to correctly intercept transmitted data, while illegitimate users cannot.

6.3. Performance and robustness evaluation of existing cipher approaches

Tables 5–7 present the results of multiple security tests done on several encryption schemes before and after the IFFT block. The correlation coefficient, ρ, indicates the similarity between the original symbols and the encrypted ones. In order to ensure a good security level, this value should be close to 0. The key sensitivity test, on the other hand, quantifies a specific scheme's sensitivity against any slight change in the key (should be close to 50%). For all tested encryption schemes, the original OFDM symbols are encrypted separately with two dynamic keys (DK1 and DK2) and the Hamming distance between the two corresponding encrypted OFDM symbols is computed. Additionally, the difference in bits between the encrypted and the original OFDM symbols should also be close to 50% to ensure the independence property.

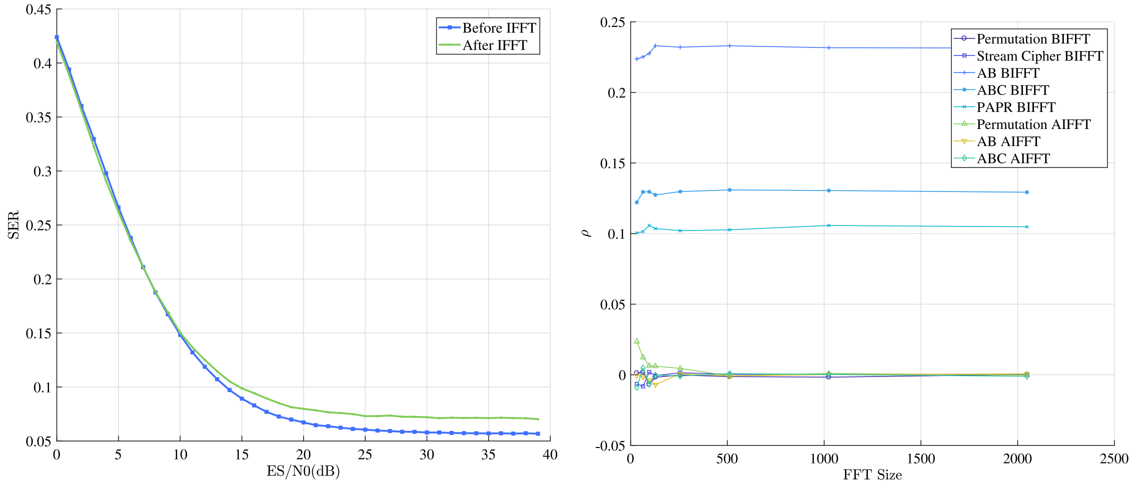
From Fig. 31 and Tables 5–7, it has been shown that there exists a trade-off between the fading performance (having various levels of noise) and the security level. More specifically, it has been proven that frequency domain encryption schemes reduce the effect of channel fading and improve the Bit Error Rate (BER), in comparison to time domain encryption schemes, which are more secure. Schemes performing encryption in the time-domain result in correlation coefficients close to the desired value $\rho = 0$, and the difference and key sensitivity values close to 50%. While those performing encryption before the IFFT block (frequency-domain) are less secure having values deviating from the desired ones. In contrast, the BER of time-domain encryption is higher than that of the frequency-domain due to error propagation resulting from IFFT diffusion.

When dealing with high-order modulation schemes, frequency-domain encryption is more suitable since the IFFT block serves as a diffusion layer in which any error in the frequency domain symbols propagates and affects multiple symbols in time domain and thus, decreasing the BER. Although high-order modulation schemes increase the data rate, they are more prone to errors due to the closely placed symbols in the constellation sets. However, this class of schemes is less secure. On the other hand, time-domain encryption is more recommended for highly sensitive and confidential data due to its robust security performance. This enhancement in security is attributed to the fact that the IFFT block introduces more randomness into the transmitted symbols, which increases the independence property between the original and the encrypted symbols (no useful information can be extracted from the encrypted symbols). This type of encryption schemes has a higher BER, especially for high-order modulation schemes.

The type/class of encryption schemes should mainly depend on the application itself whether it requires low error probability or carries sensitive information that need to be protected. Table 8 summarizes the advantages and disadvantages of Pre-OFDM and Post-OFDM encryption schemes.

Fig. 32 shows the PAPR corresponding to each scheme as a function of FFT size. As it can be depicted from both figures, performing encryption in the frequency domain results in lower PAPR than that in the time-domain. The PAPR reduction scheme, which generates several sequences and chooses the sequence with the minimum PAPR, has the best performance. This scheme, however, is computationally complex and thus, a lightweight PAPR reduction scheme should be designed taking into consideration time-domain encryption.

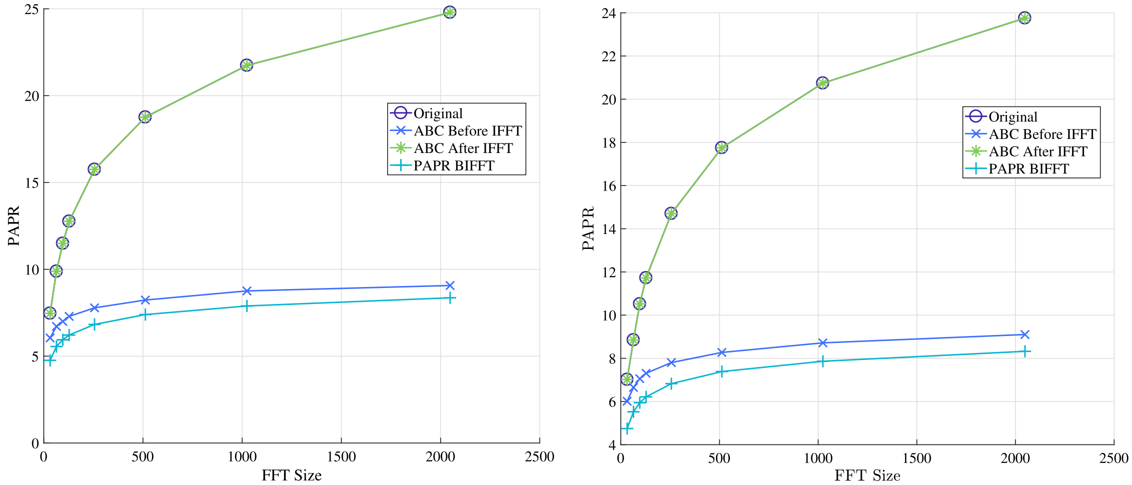
Differently, Table 7 shows the number of encrypted symbols per second, which is inversely proportional to the execution time. As it can be seen, the permutation scheme is able to encrypt the largest number of symbols within one second, and as such, requires the least execution time. This is attributed to the simplicity of the previously mentioned scheme since as the complexity increases, the execution time increases due to increased number of operations and consequently, the number of encrypted symbols per second decreases.



(a) SER

(b) ρ

Fig. 31. (a) Performance analysis of both classes of encryption schemes (pre-IFFT and post-IFFT) at different values E_s/N_0 using QPSK modulation (b) and the correlation coefficient between the original symbols and the encrypted symbols.



(a) QPSK

(b) 256-QAM

Fig. 32. The variation of PAPR as a function of FFT size for different encryption schemes for (a) QPSK modulation and (b) 256-QAM modulation.

Table 5
Statistical results of the OFDM encryption schemes using QPSK modulation.

Encryption algorithm	Permutation	Stream cipher	AB	ABC	PAPR	Perm-IFFT	AB-IFFT	ABC-IFFT
ρ	−0.0017	0.0003	−0.0003	−0.0002	−0.0002	0.0078	0.0001	−0.0001
KS	49.5517	49.9699	49.8952	49.9078	49.9992	49.5381	49.8707	49.9135
DIF	49.6078	49.9697	50.0295	50.0186	49.9647	49.5833	49.9250	49.9341

Table 6
Statistical results of the OFDM encryption schemes using 256-QAM modulation.

Encryption algorithm	Permutation	Stream cipher	AB	ABC	PAPR	Perm-IFFT	AB-IFFT	ABC-IFFT
ρ	−0.0027	0.0001	−0.5131	−0.2911	−0.1260	0.0004	0.0019	−0.0004
KS	49.5666	50.0035	12.4967	28.7656	41.6240	49.0410	49.4291	49.5202
DIF	49.6484	50.0061	12.5078	28.7306	46.4542	49.5064	49.9712	49.9907

7. Existing anti-jamming PLS solutions

Jamming attacks are one type of Denial-of-Service (DoS) attacks that threaten the performance of wireless communications, where jamming signals are intentionally emitted to disrupt communication in terms of throughput degradation and network availability, by simply occupying the channel and blocking legitimate communication [137].

Table 7
Number of OFDM symbols encrypted per second using 256-QAM modulation.

Encryption algorithm	Permutation	Stream cipher	AB	ABC	PAPR
Number of OFDM symbols per second	71 580	6966	17 323	11 458	1934

Table 8
Advantages and disadvantages of pre-OFDM and post-OFDM encryption.

Type	Pre-OFDM	Post-OFDM
Data encrypted	Frequency-domain symbols	Time-domain symbols
Advantage	Lower bit error rate	Better security since IFFT acts as a diffusion layer which increases the randomness of encrypted data
Disadvantage	Performs poorly in terms of security especially when using higher order modulation schemes	It has a higher BER. Poor performance in frequency selective fading channels.

Traditionally, there are two popular ways to mitigate jamming attacks, both of which fall under the same type of modulation technique, spread spectrum modulation. These techniques are: Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS). DSSS is similar to CDMA since it multiplies a bit sequence by a chip sequence, which is faster. As a result, the transmitted signal will be spread over a wide range of bandwidth, and consequently, interference and jamming signals will be suppressed. FHSS, on the other hand, uses narrow-band signals and hops from one frequency to another during transmission in a pseudo-random manner [138].

Another technique to mitigate jamming/interference is via beamforming whereby antenna weights in a Multi-Input Multi-Output (MIMO) system are adjusted in a way that a specific beam is directed towards the intended user. It should be noted that most anti-jamming solutions are based on the MIMO system and not on the OFDM system, which has minimal contribution in this area. Link adaptation and adaptive filtering, on the other hand, adapt transmission parameters in order to decrease the error between the received signal and the original signal, but are not effective in the presence of unpredictable or strong interference. Finally, time–frequency analysis is a technique that only reveals the power localization of the jamming signal in the time and frequency domains.

In [139], the authors present a novel jamming-resistant receiver scheme that estimates the channels of both the legitimate receiver and the jammer using an unused orthogonal pilot sequence. The transmitter picks a specific pilot sequence from a pilot codebook every τ symbols of a coherence block ($\tau < T$). It is assumed that there is at least one unused pilot sequence and that the transmitter uses a pilot hopping scheme (pseudo-random) such that the jammer is unable to know the user's current pilot sequence.

The communication between the transmitter and receiver is divided into two phases. In the first phase, the transmitter sends a pilot sequence to enable channel estimation at the receiver, and in the second phase, the transmitter sends its payload data. It is assumed that the jammer performs jamming in both phases. To eliminate jamming in the first phase, the receiver (BS) projects the received signal (legitimate user's pilot sequence and jamming signal) onto the unused orthogonal pilot sequence, so, the user's pilot signal is eliminated leaving the jamming signal only. Note that the jammer chooses a jamming signal not orthogonal to the signal present in the pilot codebook. Now, the receiver has estimated the channel of both the legitimate user and the jammer and is able to amplify the desired signal on one hand and mitigate the jamming signal on the other. It should be noted that this technique is ineffective if jamming targets the whole band.

Another defense mechanism to achieve jamming resilient OFDM systems is presented in [137]. This scheme tracks the jamming signal's direction using multiple pilots and then cancels it out. The authors rely on the fact that the jamming signal is most effective when the angle between itself and the transmitted signal is zero, that is, when both signals are aligned, and is least effective when both signals are orthogonal. In other words, the angle between the transmitted signal and jamming signal should be close to 90 degrees. As a result, the presented scheme aims to project the received signal to the direction orthogonal to that of the jamming signal. In order to do so, multiple pilots are inserted into the payload. Upon jamming, the inserted pilots, which are already known, will be corrupted (jammed). Afterwards, the jammer's channel is estimated by comparing the original pilots to the jammed ones. Consequently, the receiver will be able to know the direction of the jammed signal and will be able to rotate the received signal in a direction orthogonal to that of the jammed signal.

In [140], an anti-jamming technique is presented whereby a friendly jammer blocks unauthorized wireless transmission whenever unauthorized users are detected (by jamming), and stays silent, otherwise. In order to do so, the friendly jammer has to identify whether the ongoing transmission is authorized or not using a special preamble, which is generated by the authorized user using a shared secret key between itself and the friendly jammer. Accordingly, the friendly jammer verifies the special preamble using the secret key and launches a jamming attack to prevent unauthorized communication.

Table 9 summarizes and compares the existing anti-jamming solutions present in the literature in terms of advantages and limitations.

8. Source authentication and data integrity techniques

Data integrity is the absence of inconsistent data, which should be correct, valid, and accurate at all times [141]. The main rationale behind the concept of data integrity is to make sure that the sent data has been correctly received with no alterations or modifications, which might result from different factors such as malicious attempt, human error and hardware failure. Usually, data integrity is achieved using hash functions. A MAC (Message Authentication Code) [142], on the other hand, ensures source authenticity in which the intended sender and the correctness of the message are both verified.

The difference between a hash and a MAC is that a MAC requires a key. In a MAC operation, a user hashes the intended message and then encrypts the resulting digest with a key.

A hash function is a one-way function, which takes in a message block and outputs a fixed size message digest. A popular example of hash functions is the Secure Hash Algorithm (SHA) [143]. In order to validate the correctness of the message, the original message is hashed and the result is compared with the sent hash.

In order to achieve the full potential of PLS, data integrity and source authentication should be considered and studied thoroughly. However, there is a lack of these schemes at the physical layer in the literature. One way to do so would be to design a hash or a keyed hash that can be realized at the OFDM symbol level and append the hash at the end of each OFDM symbol. As such, the receiver can validate the integrity of the bits present in each symbol. It should be noted that there is no need for dedicated data integrity schemes since source authentication ensure both source authenticity and data integrity.

Table 9
A summary of the anti-jamming schemes presented in the literature.

Anti-jamming scheme	Pilot-index encryption	Jamming signal estimation	Pilot insertion within payload	Jamming the jammer
Advantage	Low latency and complexity	No additional overhead in terms of resources and latency	accurate estimation of the jamming signal within the jammed pilot	Prevents the jammer from sending jamming signals in real time unlike waiting for the authority's response
Limitation	If the attacker has enough power the whole bandwidth would be affected. In such a case the attacker does not need to know the pilots sent to each user	Jamming signals cannot be estimated or known since these signals are random	The jammed payload cannot be recovered since the jamming signal cannot be fully known from the jammed pilots within the payload. This technique decreases the data rate	The jammer should be able to differentiate jammers from non-jammers and an extra node monitoring the network is required
Resource and communication cost	Encryption of pilot indices and exchanging them which requires additional communication cost	No additional costs in terms of resources and communication	Using additional resources for pilot insertion in payload since pilots replace part of the intended data	Additional devices to constantly monitor the network are needed in addition to power resources to be able to send jamming signals
Complexity	Not computationally complex: encrypting pilot index not the pilot signal itself	Computationally complex to estimate a jamming signal or even a part of it	Computationally complex: (1) pilot insertion upon transmission. (2) Jammed pilot extraction upon reception and comparison with original pilots	(1) The friendly jammer should first detect whether unauthorized users have are sending (2) Generate jamming signals

9. Performance metrics

In general, secrecy can be evaluated using: (1) practical measures or (2) information-theoretic measures. The first method quantifies the security level using metrics that are observed in practical communication scenarios, whereas the second considers the limits of secrecy [132]. In this subsection, we present and discuss the practical measures only since secrecy capacity cannot be depicted or measured in practical communication scenarios, although it is a common metric for security assessment [132]. These metrics are listed and briefly discussed below:

- **Secrecy gap**: It quantifies the secrecy level based on the BER performance of both, the legitimate receiver and the eavesdropper. More specifically, it is the difference between the minimum Signal-to-Noise Ratio (SNR) of the legitimate receiver (required to achieve reliable decoding for a certain BER level) and the maximum SNR of the eavesdropper (required to achieve reliable decoding for the same BER level). This reflects the advantage that the legitimate receiver has over the eavesdropper in terms of channel quality (satisfying the secrecy notion). In [144,145] and [146], the authors present methods that exploit this metric.
- **Bit Error Rate (BER)**: BER, which is a popular measure for reliable communication, can also be used for quantifying the security performance.
- **Secure Packet Error Rate (SPER)**: SPER is the difference between the eavesdropper's PER and the legitimate receiver's PER. PER, which is the ratio of erroneously received packets to the total number of transmitted packets ($0 \leq SPER \leq 1$), was presented in [147] as a practical security metric for cross layers (PHY/MAC) security design. Typically, the ideal maximum value of SPER is 1 (desired).
- **Low Probability of Interception (LPI)/Detection (LPD)**:
  - Probability of Interception: It is the probability that the eavesdropper has further information about the transmitted signal (properties) such as the transmit filter type and inter-leaver, which is required for a reliable reception [132].
  - Probability of Detection: It is the probability of correctly detecting the presence of communication between the legitimate users, which should be as low as possible in order to ensure secure data transmission [132].

In addition to the previously mentioned metrics, we propose additional security metrics such as: the recurrence test, independence test, correlation, probability density function and key sensitivity test. These metrics are used to quantify the security and performance of traditional cryptographic algorithms. However, one can also use these metrics to evaluate the security level of PLS schemes.

10. Lessons

In this section, we summarize and highlight the important lessons learned from the literature.

Device authentication, based on PLS, can be realized by: (1) comparing channel properties at the transmitter and receiver, (2) generating a secret key from channel parameters and using this key for encryption, (3) relying on a third party authority or (4) utilizing the notion of a pre-shared secret key between communicating parties. Unlike the first two techniques which depend on channel characteristics only to authenticate devices, the fourth technique is more robust and reliable since it uses a pre-shared secret key to generate "tags", which are appended to transmitted message. It requires additional operations, however, it is more secure. Finally, relying on a third party authority for ensuring device authentication is unpractical (not a generic solution) since there should exist a high level of trust between the legitimate users and the third party authority (also vulnerable to being impersonated). As it can be depicted, current device authentication schemes are based on multiple factors such as physical channel parameters, traditional cryptography, secret, and so on. This enhances the level of accuracy and prevents authentication attacks, since physical channel parameters, in addition to cryptography, ensure robust security and provide legitimate authentication.

Key management includes key generation and key distribution. Key generation techniques, that fall under PLS, extract encryption keys directly from the channel and perform reconciliation in case of channel non-reciprocity. This approach benefits from the channel's high degree of randomness, however, does not account for the fact that the wireless medium is vulnerable to passive and active attacks. Hence, key generation techniques cannot depend on the channel characteristics alone, since this will jeopardize all subsequent operations that depend on the produced key (data confidentiality, device authentication, message integrity, etc.). As for key exchange, one can use either cryptographic protocols, jamming, or pre-coding. Cryptography is considered a good approach since it is highly secure, however, it requires additional operations and communication steps (additional costs). In contrast, jamming is not suitable in most cases due to its complexity (requires high power which might not always be feasible). Finally, pre-coding is a low complexity technique that ensures secure exchange of encryption keys.

Many works in the literature focus on enhancing the security of transmitted data using PLS. As a result, numerous techniques that achieve **data confidentiality** have emerged recently: permutation, phase encryption, artificial noise and artificial fast fading, channel-based encryption, jamming, joint PAPR reduction and encryption, power allocation and preamble encryption. Permutation, phase encryption, artificial noise and artificial fast fading, and channel-based encryption are PLS techniques that ensure high security levels using simple operations. More specifically, these methods rely on channel parameters to secure data using either permutation, random shuffling, encryption or pre-coding/pre-equalization. On the other hand, jamming, joint PAPR reduction and encryption, and power allocation are computationally complex techniques that mandate additional resources and costs. In addition, performing preamble encryption alone cannot ensure data secrecy. The first class of schemes, which is more practical and feasible than the second, mainly depend on the randomness of the shared channel. Moreover, physical channel parameters introduce dynamicity to cryptographic algorithms and protocols, which leads to enhanced security levels compared to the existing static cryptographic schemes. Here it is assumed that channel-related information are completely secure and that one cannot acquire them. However, if proven otherwise (which is a realistic assumption), the entire communication session will be leaked. Hence, additional precautions should be taken into consideration.

On the other hand, there exist no **data integrity and source authentication** PLS schemes in the literature up until now. However, ensuring data integrity at the physical layer is crucial since it prevents several integrity and source authentication attacks. This will be the focus of our future work: designing a PLS cryptographic hash function.

Finally, all **anti-jamming** techniques present in the literature depend on stringent assumptions. While some assume that jamming signals can be estimated and removed, others neglect the fact that an attacker is able to jam the entire band. Consequently, more realistic scenarios and techniques should be proposed. Moreover, there exists a strong trade-off between bandwidth and resistance against jamming. In fact, if a jammer targets a specific sub-carrier, one can hop to another subcarrier, and thus, having more bandwidth increases the resistance against jamming attacks.

11. Discussion and recommendation

Having presented the current PLS techniques, in this section, we highlight the limitations of these techniques and we suggest possible ways to overcome them.

PLS is mainly based on either cryptographic or non-cryptographic techniques. The former ones depend on the notion of encryption (keyed or keyless) and data hiding, while the latter ones do not. Non-cryptographic solutions include beamforming and jamming techniques.

Throughout the survey, we stressed on the fact that PLS schemes without a secret key cannot ensure secure transmission of data, except for jamming-based techniques. More specifically, techniques that only depend on the common properties and characteristics of the wireless channels are weak solutions since, through synchronization, eavesdroppers are able to learn the channel between any two users and therefore, are able to extract the needed information to perform data encryption, key generation and distribution, authentication and so on.

Eavesdroppers can synchronize to legitimate users by detecting the (1) exchanged pilots that are sent prior to data transmission, and (2) packet preambles. One way to overcome this problem is through preamble/pilot encryption since eavesdroppers will not be able to obtain information related to the wireless channel between users and thus, will not be able to perform synchronization.

Using physical layer parameters and a secret key ensures a dynamic structure for any proposed cryptographic algorithm and protocol. A PLS scheme can integrate and combine the physical layer properties, such as the CSI and RSS, with the secret key to generate a new dynamic secret key between communicating parties. The dynamic nature of the generated secret key is attributed to the continuous change of channel parameters. As such, different dynamic keys are produced every specific period of time.

As a result, the design of a robust, efficient and dynamic security scheme at the physical layer can guarantee the essential premise of PLS and validate its importance.

Another issue related to PLS is key generation and distribution. In the literature, many works rely on information about the shared channel between legitimate users, communicating for the first time, to extract the secret key. This is a major drawback for the same reasons mentioned previously. Channel properties are not considered private information and therefore one cannot generate a secret key based on such information alone. A set of key generation and distribution schemes can be based on a non-cryptographic approach. Jamming can be utilized in such a way that only legitimate users are able to generate and share the secret key over a wireless medium and in the presence of eavesdroppers. After generating a secret key, various services can be realized such as data integrity, source and device authentication.

Traditionally, source authentication techniques mainly depend on symmetric keys, certificates or user-specific secret (hardware or software embedded). However, with the emergence of PLS, new methods for source authentication are introduced. The dynamic characteristics and properties of the physical layer along with a secret key permit users to authenticate each other and hence prevent user/device impersonation. Again, a user can use specific channel parameters along with a secret key to authenticate the communicating party at the other end. We recommend to use two or three sub-carriers to include the MAC values in order to validate each transmitted symbol.

On the other hand, one of the main challenges in PLS is jamming attacks since finding an effective anti-jamming solution is not straightforward. In principle, jamming attacks disrupt and prevent communication between users and distort the transmitted data in a way that retrieving the original data becomes an impossible task. As a result, few techniques to solve this issue have been proposed in the literature. Currently, most techniques assume that the jammed data can be recovered once the jamming signal is estimated, however, this cannot be generalized since jamming signals are random signals and knowing a small part of a jamming signal does not help in estimating the whole signal. Therefore, a good anti-jamming technique should assume that jammed signals cannot be recovered. Another solution would be using a special device to overcome jamming attacks through power monitoring and control. This device is kept active during the whole period of communication. It can monitor the signal strength, carrier sensing time and/or the packet delivery ratio. Whenever an abnormal event occurs, this device sends an alert to the authority, which in turn stops the jammer from transmission. This approach is similar to the concept of intrusion detection/prevention systems.

Taking into consideration the aforementioned discussion, one can develop enhanced OFDM-based PLS solutions that strike a good balance between security and performance based on the random channel characteristics between two users sharing the same channel. PLS has many advantages as mentioned before and is expected to be a promising candidate to secure current and future networks and to replace traditional security solutions.

12. Conclusion

In this survey, PLS has been explored in detail and various PLS schemes have been presented and discussed thoroughly. These schemes have been summarized and compared to each other, and several limitations and challenges have been analyzed and highlighted. It has been shown that most techniques depend on the randomness of the channel only, which is not optimal in terms of system robustness and security. More specifically, using a secret key along with the random and dynamic channel properties is a promising solution to achieve modern, secure and lightweight PLS algorithms and protocols with a dynamic structure. Finally, multiple recommendations and countermeasures have been proposed to overcome the stated limitations. Our future work will focus on designing and implementing a secure data integrity PLS scheme.

Acknowledgment

This paper is supported with funds from the Maroun Semaan Faculty of Engineering and Architecture at the American University of Beirut, Lebanon.

References

[1] A. Goldsmith, Wireless Communications, Cambridge university press, 2005.

[2] V. Poor, et al., Wireless physical layer security, Proc. Nat. Acad. Sci. U. S. A. 114 (1) (2017) 19–26.

[3] W. Zhang, et al., Joint PAPR reduction and physical layer security enhancement in OFDMA-PON, IEEE Photon. Technol. Lett. 28 (9) (2016) 998–1001, http://dx.doi.org/10.1109/LPT.2016.2522965.

[4] T. Akitaya, T. Saba, Energy efficient artificial fast fading for MISO-OFDM systems, in: Proc. IEEE Global Commun. Conf. (GLOBECOM), 2015, pp. 1–6, http://dx.doi.org/10.1109/GLOCOM.2015.7417411.

[5] J. Zhang, et al., Design of an OFDM physical layer encryption scheme, IEEE Trans. Veh. Technol. 66 (3) (2017) 2114–2127.

[6] R. Fielding, et al., Hypertext transfer protocol HTTP/1.1, Tech. rep. 1999.

[7] T. Dierks, The transport layer security (TLS) protocol version 1.2.

[8] B. Forouzan, TCP/IP Protocol Suite, McGraw-Hill, Inc., 2002.

[9] J. Hamamreh, H. Arslan, Secure orthogonal transform division multiplexing (OTDM) waveform for 5g and beyond, IEEE Commun. Lett. 21 (5) (2017) 1191–1194, http://dx.doi.org/10.1109/LCOMM.2017.2651801.

[10] J. Harshan, et al., Insider-attacks on physical-layer group secret-key generation in wireless networks, in: IEEE Proc. Wireless Commun. Netw. Conf. (WCNC), IEEE, 2017, pp. 1–6.

[11] J. Zhang, et al., Verification of key generation from individual OFDM subcarrier's channel response, in: Proc. IEEE Global Commun. Conf. Workshops (GC Wkshps), 2015, pp. 1–6, http://dx.doi.org/10.1109/GLOCOMW.2015.7414111.

[12] F. Huo, G. Gong, A new efficient physical layer OFDM encryption scheme, in: Proc. IEEE Int. Conf. Computer Commun. (INFOCOM), IEEE, 2014, pp. 1024–1032.

[13] T. Akitaya, et al., Time-domain artificial noise generation technique using time-domain and frequency-domain processing for physical layer security in MIMO-OFDM systems, in: Proc. IEEE Int. Conf. Commun. (ICC), 2014, pp. 807–812, http://dx.doi.org/10.1109/ICCW.2014.6881299.

[14] X. Wu, et al., Artificial-noise-aided physical layer phase challenge-response authentication for practical OFDM transmission, IEEE Trans. Wireless Commun. 15 (10) (2016) 6611–6625, http://dx.doi.org/10.1109/TWC.2016.2586472.

[15] H. Rahbari, M. Krunz, Exploiting frame preamble waveforms to support new physical-layer functions in OFDM-Based 802.11 systems, IEEE Trans. Wireless Commun. 16 (6) (2017) 3775–3786, http://dx.doi.org/10.1109/TWC.2017.2688405.

[16] M. Soltani, et al., Achieving secure communication through pilot manipulation, in: IEEE Proc. Annual Int. Symp. on Personal, Indoor, and Mobile Radio Commun. (PIMRC), 2015, pp. 527–531, http://dx.doi.org/10.1109/PIMRC.2015.7343356.

[17] Y. Al-Moliki, M. Alresheedi, Y. Al-Harthi, Robust key generation from optical OFDM signal in indoor VLC networks, IEEE Photonics Technol. Lett. 28 (22) (2016) 2629–2632.

[18] Y. Al-Moliki, M. Alresheedi, Y. Al-Harthi, Physical-layer security against known/chosen plaintext attacks for OFDM-based VLC system, IEEE Commun. Lett. 21 (12) (2017) 2606–2609.

[19] D. Cheng, et al., A general time-domain artificial noise design for OFDM AF relay systems, in: IEEE proc. Int. Conf. Commun. China (ICCC), 2015, pp. 1–6, http://dx.doi.org/10.1109/ICCChina.2015.7448625.

[20] J. Xiong, Z. Wang, Physical layer security OFDM communication using phased array antenna, in: IEEE proc. Int. Conf. Commun. China (ICCC), 2016, pp. 1–4, http://dx.doi.org/10.1109/ICCChina.2016.7636795.

[21] Y. Tsai, et al., Effective channel perturbation based on cyclic delay for physical layer security in OFDM systems, in: IEEE Proc. Int. Conf. Inf. Sci. Electron. Electr. Eng., Vol. 2, 2014, pp. 823–827, http://dx.doi.org/10.1109/InfoSEEE.2014.6947782.

[22] A. Hajomer, et al., Secure OFDM Transmission Precoded by Chaotic Discrete Hartley Transform, IEEE Photon. J PP (99) (2017) http://dx.doi.org/10.1109/JPHOT.2017.2734817, 1–1.

[23] J.M. Hamamreh, et al., Secure pre-coding and post-coding for OFDM systems along with hardware implementation, in: IEEE proc. Int. Wireless Commun. and Mobile Comput. Conf. (IWCMC), 2017, pp. 1338–1343, http://dx.doi.org/10.1109/IWCMC.2017.7986479.

[24] F. Huo, G. Gong, XOR encryption versus phase encryption, an in-depth analysis, IEEE Trans. Electromagn. Compat. 57 (4) (2015) 903–911, http://dx.doi.org/10.1109/TEMC.2015.2390229.

[25] K. Umebayashi, et al., A study on secure pilot signal design for OFDM systems, in: Asia-Pacific Signal and Inform. Process. Association Annual Summit and Conf. (APSIPA), 2014, pp. 1–5, http://dx.doi.org/10.1109/APSIPA.2014.7041552.

[26] L. Deng, et al., Secure OFDM-PON system based on chaos and fractional fourier transform techniques, J. Lightw. Technol. 32 (15) (2014) 2629–2635, http://dx.doi.org/10.1109/JLT.2014.2331066.

[27] H. Li, et al., Secure transmission in OFDM systems by using time domain scrambling, in: IEEE proc. Veh. Technol. Conf. (VTC Spring), 2013, pp. 1–5, http://dx.doi.org/10.1109/VTCSpring.2013.6692745.

[28] L. Zhang, et al., Theory eand performance analyses in secure CO-OFDM transmission system based on two-dimensional permutation, J. Lightw. Technol 31 (1) (2013) 74–80, http://dx.doi.org/10.1109/JLT.2012.2228630.

[29] J. Lin, et al., Frequency diverse array beamforming for physical-layer security with directionally-aligned legitimate user and eavesdropper, in: European Signal Processing Conference (EUSIPCO), 2017, pp. 2166–2170, http://dx.doi.org/10.23919/EUSIPCO.2017.8081593.

[30] J. Lin, et al., Physical-layer security for proximal legitimate user and eavesdropper: a frequency diverse array beamforming approach, IEEE Trans. Inf. Forensics Secur. PP (99) (2017) http://dx.doi.org/10.1109/TIFS.2017.2765500, 1–1.

[31] G. Zhang, et al., Wireless powered cooperative jamming for secure OFDM system, IEEE Trans. Veh. Technol PP (99) (2017) http://dx.doi.org/10.1109/TVT.2017.2756877, 1–1.

[32] L. Deng, et al., Joint power and subcarrier allocation using auction games for secure multiuser OFDMA networks, in: IEEE proc. Int. Conf. Commun. China (ICCC), 2015, pp. 153–158, http://dx.doi.org/10.1109/ICCChinaW.2015.7961598.

[33] S. Sheikhzadeh, et al., Radio resource allocation for physical-layer security in OFDMA based HetNets with unknown mode of adversary, in: Iran Workshop on Communication and Information Theory (IWCIT), 2017, pp. 1–6, http://dx.doi.org/10.1109/IWCIT.2017.7947671.

[34] T. Wang, et al., Security-Coded eOFDM system based on multiorder fractional fourier transform, IEEE Commun. Lett. 20 (12) (2016) 2474–2477, http://dx.doi.org/10.1109/LCOMM.2016.2611498.

[35] K. Naito, et al., Channel state based secure wireless communication, in: IEEE Proc. Int. Conf. Computer Commun. Workshops (INFOCOM WKSHPS), 2016, pp. 828–834, http://dx.doi.org/10.1109/INFCOMW.2016.7562191.

[36] Y. Lee, et al., Secure index and data symbol modulation for OFDM-IM, IEEE Access PP (99) (2017) http://dx.doi.org/10.1109/ACCESS.2017.2768540, 1–1.

[37] J. Hamamreh, et al., OFDM-subcarrier index selection for enhancing security and reliability of 5G URLLC services, IEEE Access PP (99) (2017) http://dx.doi.org/10.1109/ACCESS.2017.2768558, 1–1.

[38] H. Li, et al., Dynamic subcarrier coordinate interleaving for eavesdropping prevention in OFDM systems, IEEE Commun. Lett. 18 (6) (2014) 1059–1062, http://dx.doi.org/10.1109/LCOMM.2014.2315648.

[39] M. Yusuf, H. Arslan, Controlled inter-carrier interference for physical layer security in OFDM systems, in: IEEE proc. Veh. Technol. Conf. (VTC-Fall), 2016, pp. 1–5, http://dx.doi.org/10.1109/VTCFall.2016.7880940.

[40] W. Zhang, et al., Hybrid time-frequency domain chaotic interleaving for physical-layer security enhancement in OFDM-PON systems, in: IEEE proc. Int. Conf. Commun. China (ICCC), IEEE, 2016, pp. 1–4.

[41] M. Sakai, et al., Intrinsic interference based physical layer encryption for OFDM/OQAM, IEEE Commun. Lett. 21 (5) (2017) 1059–1062.

[42] B. Zhang, et al., Priwhisper: enabling keyless secure acoustic communication for smartphones, IEEE Internet Things J. 1 (1) (2014) 33–45.
[43] M. Bellanger, Specification and design of a prototype filter for filter bank based multicarrier transmission, in: Acoustics, Speech, and Signal Processing, 2001. Proceedings.(ICASSP'01). 2001 IEEE International Conference on, Vol. 4, IEEE, 2001, pp. 2417–2420.
[44] B. Farhang-Boroujeny, OFDM versus filter bank multicarrier, IEEE Signal Process Mag. 28 (3) (2011) 92–112.
[45] J. Massey, Cryptography - A selective survey, Digit. Commun. 85 (1986) 3–25.
[46] M. Bloch, et al., Wireless information-theoretic security, IEEE Trans. Inform. Theory 54 (6) (2008) 2515–2534.
[47] C. Shannon, Communication theory of secrecy systems, Bell Labs Techn. J. 28 (4) (1949) 656–715.
[48] A. Wyner, The wire-tap channel, Bell Labs Techn. J. 54 (8) (1975) 1355–1387.
[49] A. Mukherjee, et al., Principles of physical layer security in multiuser wireless networks: A survey, IEEE Commun. Surveys Tuts. 16 (3) (2014) 1550–1573.
[50] M. Bloch, J. Barros, Physical-layer security cambridge univ, 2011.
[51] R. Ahlswede, et al., Common randomness in information theory and cryptography. I. Secret sharing, IEEE Trans. Inf. Theory 39 (4) (1993) 1121–1132.
[52] I. Csiszar, et al., Broadcast channels with confidential messages, IEEE Trans. Inf. Theory 24 (3) (1978) 339–348.
[53] A. Khisti, G. Wornell, Secure transmission with multiple antennas I: The MISOME wiretap channel, IEEE Trans. Inf. Theory 56 (7) (2010) 3088–3104.
[54] J. Liu, et al., Optimal power allocation for achieving perfect secrecy capacity in MIMO wire-tap channels, in: IEEE proc. Inf. Sci. and Syst., IEEE, 2009, pp. 606–611.
[55] H. Li, et al., Eavesdropping-resilient OFDM system using sorted subcarrier interleaving, IEEE Trans. Wireless Commun. 14 (2) (2015) 1155–1165.
[56] D. Ng, et al., Energy-efficient eresource allocation for secure OFDMA systems, IEEE Trans. Veh. Technol. 61 (6) (2012) 2572–2585.
[57] E. Guvenkaya, H. Arslan, Secure communication in frequency selective channels with fade-avoiding subchannel usage, in: Proc. IEEE Int. Conf. Commun. (ICC), IEEE, 2014, pp. 813–818.
[58] M. Dworkin, Recommendation for block cipher modes of operation: methods and techniques, Tech. rep.,, DTIC Document, 2001.
[59] C. Shannon, Communication theory of secrecy systems, Bell Syst. Tech. J. 28 (1949) 656–715.
[60] C. Paar, J. Pelzl, Understanding Cryptography: a Textbook for Students and Practitioners, Springer Science & Business Media, 2009.
[61] T. Kwon, et al., Design and implementation of a simulator based on a cross-layer protocol between MAC and PHY layers in a WiBro Compatible. IEEE 802.16 e OFDMA system, IEEE Commun. Mag. 43 (12) (2005) 136–146.
[62] D. Swift, A practical application of SIM/SEM/SIEM automating threat identification, Paper, SANS Infosec Reading Room, The SANS.
[63] B. Saltzberg, Performance of an efficient parallel data transmission system, IEEE Trans. on Commun. Technol. 15 (6) (1967) 805–811.
[64] R. Chang, Synthesis of band-limited orthogonal signals for multichannel data transmission, Bell Labs Tech. J. 45 (10) (1966) 1775–1796.
[65] J. Bingham, Multicarrier modulation for data transmission: An idea whose time has come, IEEE Commun. Mag. 28 (5) (1990) 5–14.
[66] M. Schwartz, Mobile Wireless Communications, Cambridge University Press, 2004.
[67] R. Prasad, OFDM for Wireless Communications Systems, Artech House, 2004.
[68] Concepts of orthogonal frequency division multiplexing (OFDM) and 802.11 WLAN, http://rfmw.em.keysight.com/wireless/helpfiles/89600b/webhelp/subsystems/wlan-ofdm/content/ofdm_basicprinciplesoverview.htm, (Accessed on 01/04/2018).
[69] 802.11 OFDM WLAN Overview, http://rfmw.em.keysight.com/wireless/helpfiles/89600b/webhelp/subsystems/wlan-ofdm/content/ofdm_80211-overview.htm, (Accessed on 01/04/2018).
[70] I. C. S. L. S. Committee, et al., Wireless LAN medium access control (MAC) and physical layer (PHY), specifications, IEEE Standard 802.11-1997.
[71] R. Franzin, et al., A performance comparison between OFDM and FBMC in PLC applications, in: IEEE International Conference on Ecuador Technical Chapters Meeting (ETCM), IEEE, 2017.
[72] V. Moles-Cases, et al., A comparison of OFDM, QAM-FBMC, and OQAM-FBMC waveforms subject to phase noise, in: Proc. IEEE Int. Conf. Commun. (ICC), IEEE, 2017, pp. 1–6.
[73] Q. He, A. Schmeink, Comparison and evaluation between FBMC and OFDM systems, in: Proc. Int. ITG Workshop on Smart Antennas (WSA), VDE, 2015, pp. 1–7.
[74] A. Roessler, 5G waveform candidates application note, Rohde&Schwarz, Munich, Germany, Tech. Rep. 1MA271.
[75] Y. Cao, et al., A survey of emerging m2m systems: context, task and objective, IEEE Internet Things J. 3 (6) (2016) 1246–1258.
[76] A. Asadi, et al., A survey on device-to-device communication in cellular networks, IEEE Commun. Surv. Tut. 16 (4) (2014) 1801–1819.
[77] L. Atzori, et al., The internet of things: A survey, Comput. Netw. 54 (15) (2010) 2787–2805.
[78] S. Chen, et al., Vehicle-to-Everything (v2x) services supported by LTE-based systems and 5G, IEEE Commun. Stand. Mag. 1 (2) (2017) 70–76.
[79] S.O. Jr, The wireless industry begins to embrace femtocells, Computer 41 (7) (2008).
[80] X. Wu, et al., Physical-layer authentication for multi-carrier transmission, IEEE Commun. Lett. 19 (1) (2015) 74–77.
[81] F. Liu, et al., A two dimensional quantization algorithm for CIR-based physical layer authentication, in: Proc. IEEE Int. Conf. Commun. (ICC), 2013, pp. 4724–4728, http://dx.doi.org/10.1109/ICC.2013.6655319.
[82] M. Pospl, R. Mark, Experimental study of wireless transceiver authentication using carrier frequency offset monitoring, in: International Conference Radioelektronika (RADIOELEKTRONIKA), 2015, pp. 335–338, http://dx.doi.org/10.1109/RADIOELEK.2015.7129060.
[83] M. Liu, et al., TBAS: Enhancing wi-fi authentication by actively eliciting channel state information, in: IEEE Int. Conf. Sensing, Commun. and Netw. (SECON), 2016, pp. 1–9, http://dx.doi.org/10.1109/SAHCN.2016.7733021.
[84] C. Dai, et al., Physical layer authentication algorithm based on SVM, in: IEEE proc. Int. Conf. Commun. China (ICCC), IEEE, 2016, pp. 1597–1601.
[85] H. Wen, et al., A novel framework for message authentication in vehicular communication networks, in: Proc. IEEE Global Commun. Conf. (GLOBECOM), IEEE, 2009, pp. 1–6.
[86] G. Caparra, et al., Energy-based anchor node selection for IoT physical layer authentication, in: Proc. IEEE Int. Conf. Commun. (ICC), IEEE, 2016, pp. 1–6.
[87] J. Zhang, et al., Using basis expansion model for physical layer authentication in time-variant system, in: IEEE Proc. Commun. Netw. Security (CNS), IEEE, 2016, pp. 348–349.
[88] A. Mahmood, et al., Channel impulse response-based distributed physical layer authentication, arXiv preprint arXiv:1703.08559.
[89] W. Wang, et al., Privacy-Preserving location authentication in Wi-Fi networks using fine-grained physical layer signatures, IEEE Trans. Wireless Commun. 15 (2) (2016) 1218–1225, http://dx.doi.org/10.1109/TWC.2015.2487453.
[90] X. Du, et al., Physical layer challenge-response authentication in wireless networks with relay, in: Proc. IEEE Int. Conf. Computer Commun. (INFOCOM), 2014, pp. 1276–1284, http://dx.doi.org/10.1109/INFOCOM.2014.6848060.
[91] G. Verma, et al., Physical layer authentication via fingerprint embedding using software-defined radios, IEEE Access 3 (2015) 81–88.
[92] X. Wu, et al., A channel coding approach for physical-layer authentication, in: IEEE Proc. Wireless Commun. Sig. Process. (WCSP), IEEE, 2016, pp. 1–5.
[93] A. Amanna, et al., Realizing physical layer authentication using constellation perturbation on a software-defined radio testbed, in: IEEE Proc. Military Commun. Conf. (MILCOM), IEEE, 2016, pp. 1207–1212.
[94] X. Fang, et al., Towards PHY-aided authentication via weighted fractional fourier transform, in: IEEE proc. Veh. Technol. Conf. (VTC-Fall), IEEE, 2016, pp. 1–5.
[95] J. Yang, et al., A physical-layer authentication scheme based on hash method, in: IEEE proc. Int. Conf. Commun. China (ICCC), IEEE, 2015, pp. 99–104.
[96] D. Xu, P. Ren, J. Ritcey, Y. Wang, Code-frequency block group coding for anti-spoofing pilot authentication in multi-antenna ofdm systems, IEEE Trans. Inf. Forensics Secur. 13 (7) (2018) 1778–1793.
[97] J. Zhang, et al., Key generation from wireless channels: A review, IEEE Access 4 (2016) 614–626.
[98] Z. Rezki, et al., Secret key agreement: fundamental limits and practical challenges, IEEE Wireless Commun. (2017).
[99] J. Zhang, et al., Efficient key generation by exploiting randomness from channel responses of individual OFDM subcarriers, IEEE Trans. Commun. 64 (6) (2016) 2578–2588, http://dx.doi.org/10.1109/TCOMM.2016.2552165.
[100] C. Sahin, et al., Secure and robust symmetric key generation using physical layer techniques under various wireless environments, in: IEEE Radio and Wireless Symposium (RWS), IEEE, 2016, pp. 211–214.
[101] Y. Peng, et al., Secret key generation based on estimated channel state information for TDD-OFDM systems over fading channels, IEEE Trans. Wireless Commun. 16 (8) (2017) 5176–5186, http://dx.doi.org/10.1109/TWC.2017.2706657.
[102] A. Mazin, et al., Secure key management for 5G physical layer security, in: IEEE proc. Wireless Microw. Technol. Conf. (WAMICON), IEEE, 2017, pp. 1–5.
[103] Y.M. Al-Moliki, et al., Robust key generation from optical OFDM signal in indoor VLC networks, IEEE Photon. Technol. Lett. 28 (22) (2016) 2629–2632, http://dx.doi.org/10.1109/LPT.2016.2609683.
[104] R. Horstmeyer, et al., Physical key-protected one time pad, US Patent 9, 054, 871 (Jun. 9 2015).
[105] J. Guajardo, et al., FPGA intrinsic PUFs and their use for IP protection, in: CHES, Vol. 4727, Springer, 2007, pp. 63–80.
[106] L. Bolotnyy, G. Robins, Physically unclonable function-based security and privacy in RFID systems, in: IEEE Proc. Int. Conf. Pervasive Comput. Commun. (PerCom'07), IEEE, 2007, pp. 211–220.
[107] R. Pappu, et al., Physical one-way functions, Science 297 (5589) (2002) 2026–2030.
[108] P. Tuyls, et al., Security with Noisy Data: on Private Biometrics, Secure key Storage and Anti-counterfeiting, Springer Science & Business Media, 2007.

[109] S. Gollakota, D. Katabi, Physical layer wireless security made fast and channel independent, in: Proc. IEEE Int. Conf. Computer Commun. (INFOCOM), IEEE, 2011, pp. 1125–1133.

[110] J. Zhang, et al., Securing wireless communications of the internet of things from the physical layer, an overview, Entropy 19 (8) (2017) 420.

[111] H. Liu, et al., Fast and practical secret key extraction by exploiting channel response, in: Proc. IEEE Int. Conf. Computer Commun. (INFOCOM), 2013, pp. 3048–3056, http://dx.doi.org/10.1109/INFCOM.2013.6567117.

[112] Y. Zhang, et al., An over-the-air key establishment protocol using keyless cryptography, Future Gener. Comput. Syst. (2016).

[113] A. Badawy, et al., Channel secondary random process for robust secret key generation, in: IEEE proc. Int. Wireless Commun. and Mobile Comput. Conf. (IWCMC), 2015, pp. 114–119, http://dx.doi.org/10.1109/IWCMC.2015.7289067.

[114] A. Badawy, et al., Unleashing the secure potential of the wireless physical layer: Secret key generation methods, Phys. Commun. 19 (2016) 1–10.

[115] R. Guillaume, et al., Fair comparison and evaluation of quantization schemes for PHY-based key generation, in: Proc. Int. OFDM Workshop (InOWo'14), 2014, pp. 1–5.

[116] A. Saad, et al., Comparative simulation for physical layer key generation methods, in: IEEE proc. Int. Wireless Commun. and Mobile Comput. Conf. (IWCMC), IEEE, 2015, pp. 120–125.

[117] O. Gunlu, et al., Reliable secret-key binding for physical unclonable functions with transform coding, in: IEEE Proc. Global Cpnf. Signal Inf. Process. (GlobalSIP), IEEE, 2016, pp. 986–991.

[118] Z. Mahmood, et al., Lightweight two-level session key management for end user authentication in internet of things, in: Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2016 IEEE International Conference on, IEEE, 2016, pp. 323–327.

[119] W. Xi, et al., KEEP: Fast secret key extraction protocol for D2D communication, in: IEEE Int. Symp. of Quality of Service (IWQoS), 2014, pp. 350–359, http://dx.doi.org/10.1109/IWQoS.2014.6914340.

[120] J. Li, et al., Analysis of non-reciprocity factors in extracting secret key from wireless channels for practical indoor scenarios, in: IEEE proc. Int. Conf. Commun. China (ICCC), 2016, pp. 227–231, http://dx.doi.org/10.1109/CompComm.2016.7924698.

[121] WARP Project, http://warpproject.org/trac (Accessed on 01/04/2018).

[122] P. Luo, et al., Threat on physical layer security: Side channel vs. wiretap channel, in: IEEE Proc. Int. Conf. Comput. Science Eng. (CSE), IEEE, 2013, pp. 295–300.

[123] F. Huo, G. Gong, A new efficient physical layer OFDM encryption scheme, in: Proc. IEEE Int. Conf. Computer Commun. (INFOCOM), Toronto, ON, Canada, 2014, pp. 1024–1032.

[124] H. Furqan, J. Hamamreh, H. Arslan, Enhancing physical layer security of OFDM systems using channel shortening, in: IEEE Proc. International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), IEEE, 2017, pp. 1–5.

[125] L. Chen, et al., Fast power allocation for secure communication with full-duplex radio, IEEE Trans. Signal Process. 65 (14) (2017) 3846–3861, http://dx.doi.org/10.1109/TSP.2017.2701318.

[126] M. Zhang, Y. Liu, Energy Harvesting for Physical-Layer Security in OFDMA Networks, IEEE Trans. Inf. Forensics Secur. 11 (1) (2016) 154–162, http://dx.doi.org/10.1109/TIFS.2015.2481797.

[127] H. Qin, et al., Power allocation and time-domain artificial noise design for wiretap OFDM with discrete inputs, IEEE Trans. Wirel. Commun. 12 (6) (2013) 2717–2729.

[128] S. Karachontzitis, et al., Security-Aware max-min resource allocation in multiuser OFDMA downlink, IEEETrans. Inf. Forensics Secur. 10 (3) (2015) 529–542, http://dx.doi.org/10.1109/TIFS.2014.2384392.

[129] R. Saini, et al., Jammer-Assisted resource allocation in secure OFDMA with untrusted users, IEEETrans. Inf. Forensics Secur. 11 (5) (2016) 1055–1070, http://dx.doi.org/10.1109/TIFS.2016.2516912.

[130] N. Mokari, et al., Secure robust ergodic uplink resource allocation in relay-assisted cognitive radio networks, IEEE Trans. Signal Process. 63 (2) (2015) 291–304, http://dx.doi.org/10.1109/TSP.2014.2370949.

[131] Y. Xiao, et al., PAPR reduction based on chaos combined with SLM technique in optical OFDM IM/DD system, Opt. Fiber Technol. 21 (2015) 81–86.

[132] E. Güvenkaya, J. Hamamreh, H. Arslan, On physical-layer concepts and metrics in secure signal transmission, Phys. Commun. 25 (2017) 14–25.

[133] Z. Ankaralı, H. Arslan, Cyclic feature suppression for physical layer security, Phys. Commun. 25 (2017) 588–597.

[134] A. Sheikholeslami, D. Goeckel, H. Pishro-Nik, Everlasting secrecy by exploiting non-idealities of the eavesdropper's receiver, IEEE J. Sel. Areas Commun. 31 (9) (2013) 1828–1839.

[135] A. Boulogeorgos, D. Karas, G. Karagiannidis, How much does I/Q imbalance affect secrecy capacity?, IEEE Commun. Lett. 20 (7) (2016) 1305–1308.

[136] J. Zhu, R. Schober, V. Bhargava, Physical layer security for massive MIMO systems impaired by phase noise., in: SPAWC, 2016, pp. 1–5.

[137] Q. Yan, et al., Jamming resilient communication using MIMO interference cancellation, IEEE Trans. Inf. Forensics Security 11 (7) (2016) 1486–1499, http://dx.doi.org/10.1109/TIFS.2016.2535906.

[138] E. McCune, DSSS vs. FHSS narrowband interference performance issues, RF Sign. Proces. Mag. (2000).

[139] T. Do, et al., Jamming-Resistant receivers for the massive MIMO uplink, IEEE Trans. Inf. Forensics Secur. PP (99) (2017) http://dx.doi.org/10.1109/TIFS.2017.2746007, 1–1.

[140] W. Shen, et al., No time to demodulate-fast physical layer verification of friendly jamming, in: IEEE Proc. Military Commun. Conf. (MILCOM), IEEE, 2015, pp. 653–658.

[141] P. Ponniah, Database Design and Development: an Essential Guide for IT professionals, Wiley Online Library, 2003.

[142] T. Krovetz, UMAC: Message authentication code using universal hashing.

[143] M. Bhatia, et al., OSPFv2 HMAC-SHA cryptographic authentication, Tech. rep., 2009.

[144] D. Klinc, et al., LDPC for physical layer security, in: Proc. IEEE Global Commun. Conf. (GLOBECOM), IEEE, 2009, pp. 1–6.

[145] M. Baldi, M. Bianchi, F. Chiaraluce, Non-systematic codes for physical layer security, in: IEEE Proc. Information Theory Workshop (ITW), IEEE, 2010, pp. 1–5.

[146] N. Maturo, et al., Security gap assessment for the fast fading wiretap channel, in: IEEE Proc. Conf. Telecommunications (ICT), IEEE, 2013, pp. 1–5.

[147] J. Hamamreh, M. Yusuf, T. Baykas, H. Arslan, Cross MAC/PHY layer security design using ARQ with MRC and adaptive modulation, in: IEEE Proc. Wireless Communications and Networking Conference (WCNC), IEEE, 2016, pp. 1–7.

Reem Melki received her BS degree in electrical and computer engineering from the Rafik Hariri University in 2013, and the MS degree in 2015. She is currently a Ph.D. student at the American University of Beirut (AUB). Her main areas of research interests include security and privacy in wireless and mobile communication.

Hassan Noura received his degree in Computer and Communication Engineering from the IUL University in 2008, Lebanon, and his Ph.D. degree from Polytech'Nantes in 2012, France. In 2013, Noura joined Paris-Sud XI University, as a postdoctoral researcher, after that as research engineering at CEA, Grenoble. After that, he joined QMIC in 2015 and Telecom ParisTech in 2016. Recently, he gets his HDR in 2016 and joins AUB in 2017. His research interests include cryptography, network security, secure network coding, secure multimedia and secure distributed system.

Mohammad M. Mansour received the B.E. (Hons.) and the M.E. degrees in computer and communications engineering from the American University of Beirut (AUB), Beirut, Lebanon, in 1996 and 1998, respectively, and the M.S. degree in mathematics and the Ph.D. degree in electrical engineering from the University of Illinois at Urbana–Champaign (UIUC), Champaign, IL, USA, in 2002 and 2003, respectively.

He was a Visiting Researcher at Qualcomm, San Jose, CA, USA, in summer of 2016, where he worked on baseband receiver architectures for the IEEE 802.11ax standard. He was a Visiting Researcher at Broadcom, Sunnyvale, CA, USA, from 2012 to 2014, where he worked on the physical layer SoC architecture and algorithm development for LTE-Advanced baseband receivers. He was on research leave with Qualcomm Flarion Technologies in Bridgewater, NJ, USA, from 2006 to 2008, where he worked on modem design and implementation for 3GPP-LTE, 3GPP2-UMB, and peer-to-peer wireless networking physical layer SoC architecture and algorithm development. He was a Research Assistant at the Coordinated Science Laboratory (CSL), UIUC, from 1998 to 2003. He worked at National Semiconductor Corporation, San Francisco, CA, with the Wireless Research group in 2000. He was a Research Assistant with the Department of Electrical and Computer Engineering, AUB, in 1997, and a Teaching Assistant in 1996. He joined as a faculty member with the Department of Electrical and Computer Engineering, AUB, in 2003, where he is currently a Professor. His research interests are in the area of energy-efficient and high-performance VLSI circuits, architectures, algorithms, and systems for computing, security, communications, and signal processing.

Prof. Mansour is a member of the Design and Implementation of Signal Processing Systems (DISPS) Technical Committee Advisory Board of the IEEE Signal Processing Society. He served as a member of the DISPS Technical Committee from 2006 to 2013. He served as an Associate Editor for IEEE T RANSACTIONS ON C IRCUITS AND S YSTEMS II (TCAS-II) from 2008 to 2013, as an Associate Editor for the IEEE S IGNAL P ROCESSING L ETTERS from 2012 to 2016, and as an Associate Editor of the IEEE T RANSACTIONS ON VLSI S YSTEMS from 2011 to 2016. He served as the Technical Co-Chair of the IEEE Workshop on Signal Processing Systems in 2011, and as a member of the Technical Program Committee of various international conferences and workshops. He was the recipient of the PHI Kappa PHI Honor Society Award twice in 2000 and 2001, and the recipient of the Hewlett Foundation Fellowship Award in 2006. He has seven issued U.S. patents.

Ali Chehab received his Bachelor degree in EE from AUB in 1987, the MasterâĂŹs degree in EE from Syracuse University in 1989, and the Ph.D. degree in ECE from the University of North Carolina at Charlotte, in 2002. From 1989 to 1998, he was a lecturer in the ECE Department at AUB. He rejoined the ECE Department at AUB as an Assistant Professor in 2002, became Full Professor in 2014. He received the AUB Teaching Excellence Award in 2007. He teaches courses in Programming, Electronics, Digital Systems Design, Computer Organization, Cryptography, and Digital Systems Testing. His research interests include: Wireless Communications Security, Cloud Computing Security, Multimedia Security, Trust in Distributed Computing, Low Energy VLSI Design, and VLSI Testing. He has about 210 publications. He is a senior member of IEEE and a senior member of ACM.