This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2018.2878035, IEEE Communications Surveys & Tutorials

Classifications and Applications of Physical Layer Security Techniques for Confidentiality: A Comprehensive Survey

Jehad M. Hamamreh, Haji M. Furqan, and Huseyin Arslan, *Fellow, IEEE*

***Abstract*—Physical layer security (PLS) has emerged as a new concept and powerful alternative that can complement and may even replace encryption-based approaches, which entail many hurdles and practical problems for future wireless systems. The basic idea of PLS is to exploit the characteristics of the wireless channel and its impairments including noise, fading, interference, dispersion, diversity, etc. in order to ensure the ability of the intended user to successfully perform data decoding while preventing eavesdroppers from doing so. Thus, the main design goal of PLS is to increase the performance difference between the link of the legitimate receiver and that of the eavesdropper by using well-designed transmission schemes.**

In this survey, we propose a conceptual, generic, and expandable framework for classifying the existing PLS techniques against wireless passive eavesdropping. In this flexible framework, the security techniques that we comprehensively review in this treatise are divided into two primary approaches: signal-to-interference-plus-noise ratio (SINR)-based approach and complexity-based approach. The first approach is classified into three major categories: first, secrecy channel codes-based schemes; second, security techniques based on channel adaptation; third, schemes based on injecting interfering artificial (noise/jamming) signals along with the transmitted information signals. The second approach (complexity-based), which is associated with the mechanisms of extracting secret sequences from the shared channel, is classified into two main categories based on which layer the secret sequence obtained by channel quantization is applied on. The techniques belonging to each one of these categories are divided and classified into three main signal domains: time, frequency and space. For each one of these domains, several examples are given and illustrated along with the review of the state-of-the-art security advances in each domain. Moreover, the advantages and disadvantages of each approach alongside the lessons learned from existing research works are stated and discussed.

The recent applications of PLS techniques to different emerging communication systems such as visible light communication (VLC), body area network (BAN), power line communication (PLC), Internet of things (IoT), smart grid, mm-Wave, cognitive radio (CR), vehicular ad-hoc network (VANET), unmanned aerial vehicle (UAV), ultra-wideband (UWB), device-to-device (D2D), radio-frequency identification (RFID), index modulation (IM) and 5G non-orthogonal multiple access (NOMA) based-systems, are also reviewed and discussed. The paper is concluded with recommendations and future research directions for designing robust, efficient and strong security methods for current and future wireless systems.

J. Hamamreh is with the Department of Electrical and Electronics Engineering, Antalya Bilim University, Antalya, 07468, Turkey. M. Furqan and H. Arslan are with the Department of Electrical and Electronics Engineering, Istanbul Medipol University, Istanbul, 34810, Turkey. H. Arslan is also with the Department of Electrical Engineering, University of South Florida, Tampa, FL, 33620, USA. (Corresponding author: Jehad M. Hamamreh, email: jehad.hamamreh@gmail.com; jehad.hamamreh@antalya.edu.tr).

***Index Terms*—Physical layer security, cross-layer security, eavesdropping, channel secrecy codes, adaptation, interfering signals, artificial noise, jamming, secret keys, signal domains: time, frequency and space, VLC, BAN, PLC, IoT, smart grid, mm-Wave, cognitive radio, vehicular, ,UAV, UWB, D2D, RFID, index modulation, spatial modulation, 5G systems, OFDM, MIMO, Relay, NOMA, full-duplex, TDD.**

NOMENCLATURES

ACK	Acknowledgment
AF	Amplify and forward
AFF	Artificial fast fading
AN	Artificial Noise
ARQ	Automatic Repeat Request
ASM	Antenna Subset Modulation
AST	Antenna Subset Transmission
AWGN	Additive white Gaussian noise
BAN	Body Area Network
BER	Bit Error Rate
CCRN	Cooperative Cognitive Radio Network
CoMP	Cooperative Multi-Point
CP	Cyclic Prefix
CR	Cognitive Radio
CRN	Cognitive Radio Network
CSI	Channel State Information
CSIT	Channel State Information at the Transmitter
DAS	Distributed Antenna System
DM	Directional Modulation
DPA	Distributed Phase Alignment
ECN	Eavesdropper Channel Nulling
FDD	Frequency Division Duplex
FFT	Fast Fourier Transform
GSVD	Generalized Singular Value Decomposition
HARQ	Hybrid Automatic Retransmission Request
IMD	Implantable Medical Devices
INR	Incremental redundancy
IoT	Internet of Things
LDPC	Low-Density Parity-Check
LPI	Low Probability of Interception
MIMO	Multiple-Input Multiple-Output
MISO	Multiple-Input Single-Output
MISOME	Multiple-Input Single-Output Multiple-Eavesdropper
ML	Maximum-likelihood
mm-Wave	Millimetre Wave
MRC	Maximum Ratio Combining

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2018.2878035, IEEE Communications Surveys & Tutorials

MRT . . Maximum Ratio Transmitting
MSE . . Minimize Mean Square Error
NACK . Negative Acknowledgment
NFDAM Near-Field Direct Antenna Modulation
NOMA . Non-Orthogonal Multiple Access
OFDM . Orthogonal Frequency Division Multiplexing
OFDMA Orthogonal Frequency-Division Multiple Access
OSJS . . Optimal Stopping based Jammer Selection
OTDM . Orthogonal Transform Division Multiplexing
PAPR . . Peak to Average Power Ratio
PER . . Packet Error Rate
PLC . . Power Line Communication
PLS . . . Physical Layer Security
PMI . . Pre-coding Matrix Indicator
PsaaS . . Physical Security as a Service
PU . . . Primary User
QoS . . . Quality of Service
RFID . . Radio-Frequency Identification
RI . . . Rank Indicator
RSSI . . Received Signal Strength indicator
RTD . . Repetition Time Diversity
Rx . . . Receiver
SAH . . Silent Antenna Hopping
SARA . Secrecy Adaptation and Rate Adaptation
SC . . . Selection Combining
SOP . . Secrecy Outage Performance
SIC . . . Successive Interference Cancellation
SIMO . Single-Input Multiple-Output
SINR . . Signal-to-Interference-and-Noise Ratio
SISO . . Single-Input Single-Output
SJ . . . . Selection jammer
SKR . . Secret Key Rate
SM . . . Spatial Modulation
SNR . . Signal-to-Noise Ratio
SOP . . Secrecy Outage Performance
SU . . . Secondary User
TDD . . Time Division Duplex
TDMA . Time-Division Multiple Access
Tx . . . Transmitter
URLLC Ultra-Reliable Low Latency Communications
VANET . Vehicular Ad-Hoc Networks
VLC . . Visible Light Communication
V2I . . . Vehicle to infrastructure
V2V . . Vehicle to vehicle
WDM . Wavelength division multiplexing
ZF . . . Zero Forcing
ZFB . . Zero Forcing Beamforming
5G . . . Fifth-Generation

CONTENTS

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2018.2878035, IEEE Communications Surveys & Tutorials

I. Introduction

WIRELESS communication services are enormously increasing day by day as a consequence of the massive spread in wireless devices featured by high mobility and ease of use. Moreover, the surge in wireless data communication is primarily driven by the huge amount of beneficial applications customized for mobile users. Since wireless media is becoming the dominant access for most of the Internet-based services, serious security risks appear on the service-carrying wireless signals and waves because of their broadcast nature.

Thus, new security requirements have urgently been demanded. Specifically, users require confidential transmission for their generated wireless data, such as their important sensitive messages, calls, videos, financial transactions, etc. As a matter of fact, strongly secure communication systems are desirable to be implemented without just relying on the traditional cryptographic key-based sharing approaches, which are mostly dependent Shannon's security model [1].

To this end, physical layer security (PLS)[1] [2], the key driving factor for research besides capacity, reliability and delay, emerges as a promising and revolutionizing concept to address the eavesdropping security problem [3]–[6]. The driving motivations behind PLS research can be summarized by the following five practical security problems.

First, the key management, distribution, and maintenance processes for the legitimate parties are extremely challenging, especially in large-scale heterogeneous and decentralized wireless networks.

Second, longer key length, which is desirable to increase the confidentiality level, results in more waste of resources, which are needed for sharing, storing and managing the keys properly; apart from the fact that implementing security methods with Shannon's perfect secrecy[2] using one time pad method, which requires secret key of length equal to the data itself, is impractical in today's data volume.

Third, the fast developments and advances in computing power devices reveal the fact that current secret key-based techniques, which are based on the assumption that the eavesdropper has limited computational power capabilities, can be cracked, no matter how much mathematically complex they are, especially when quantum computing becomes real.

Fourth, the emergence of new wireless technologies like Internet of Things (IoT), massive machine-type communication (mMTC), 5G-Tactile Internet, vehicular communication for autonomous driving, remote surgery, instant control for sensitive IoT actuators, etc. makes current encryption-based methods unsuitable since these kind of technologies are naturally delay-sensitive, power-limited, and processing-restricted.

Fifth, users with sensitive applications like those related to financial and personal secret information can never compromise security, even if it becomes at the expense of slight degradation in other performance measures like throughput and reliability. In the near future, users are anticipated to even be willing and ready to pay extra charges just for the sake of completely ensuring the security of their important services. Thus, Physical Security as a Service (PSaaS) is expected to be one of the future coming killer applications for mobile service providers, where users can be charged a little more for providing them with strong, perfect secure services.

The story of modern security starts from Shannon, who laid down the foundation of secrecy systems in his seminal paper [1]. Although Shannon-based works (i.e., cryptography-based methods that assume noiseless channel at both the legitimate and eavesdropper sides) have dominantly been applied to secure communication systems using shared secret keys, they have got serious drawbacks and issues, which are basically the motivations for the PLS research. These issues are basically the aforementioned first four points summarized in the previous paragraphs. As a consequence of the many issues associated with cryptographic-based security, key-less information-theoretic security has emerged as a desirable and promising solution to address most (if not all) of the aforementioned issues. In Wyner's work [2], which constitutes the foundation and starting point of the research on PLS, it was explained that confidential communication between legitimate users is possible without sharing a secret key if the eavesdropper's (Eve's) channel is a degraded (much noisier) version of the intended receiver's (Bob) channel. Accordingly, channel-dependent stochastic encoders, which generate random secrecy codes, were used to achieve confidentiality by exploiting the channel without using shared secret keys.

Similar to Shannon-based works, Wyner-based studies have also obtained their own drawbacks and limitations, which can be summarized as follows: 1) Eve is always assumed to have a degraded channel compared to Bob, i.e., Eve's signal-to-interference-and-noise ratio (SINR) must be lower than that of Bob. However, In practical scenarios, due to the uncertain location, random fading, and broadcast nature of the wireless channel, Eve's channel condition, represented by the SINR, can be comparable to or even better than Bob's one, especially when Eve is closer to the transmitter than Bob; therefore, Wyner-based methods become inapplicable in such scenarios. 2) Secrecy can be achieved in most cases at the expense of

[1]It should be emphasized that the "physical layer security" phrase used in this survey paper is meant to represent the physical layer security techniques used for providing **confidentiality** throughout the whole paper.

[2]It is an information-theoretic notion which indicates the highest security level, where the secrecy capacity is equal to the capacity of the main channel for key-less-based methods or the length of the secret key is equal to the length of the transmitted data for key-based methods, resulting in a perfect secrecy in which there is no information leakage to Eve.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2018.2878035, IEEE Communications Surveys & Tutorials

capacity and throughput reduction (i.e., there is an intrinsic trade-off between capacity and secrecy).

Inspired by Wyner's work, the characterization and investigation of the achievable secrecy capacity against eavesdropping were studied from an information-theoretic point of view for different channel types, communication scenarios, and under various assumptions on the availability of channel state information (CSI). These studies were extensively surveyed and reported in several recent survey papers [4]–[7] and books on physical layer security [8]–[12]. Our survey paper is different from the aforementioned surveys and books in the sense that it is the first to propose and establish a taxonomy framework that can classify all the existing PLS techniques in a coherent, conceptual and meaningful (easy to understand) way. Besides, it inclusively discusses and comprehensibly reviews the applications of PLS to thirteen different areas of communication systems for the first time in the literature.

Motivation: We have thoroughly explored and investigated the aforementioned elegant surveys alongside other topic-specific tutorials [3], [13]–[24]; and noticed that most of these surveys review the previously published studies on PLS based on communication scenarios, channel types and conditions, or system configurations (with more focus on information theoretical studies) with the goal to span and cover most of the research papers published on PLS in an inclusive methodological manner. More precisely, in most of the available well-known PLS surveys such as [4], [5], [20], and [7], one can clearly notice that the common structure adopted in reviewing the PLS papers available in the literature is more or less scenario-dependent, where the studies are divided into different wiretap channels and scenarios of the following main types: 1) single antenna, 2) multi-antenna, 3) relay, 4) multiuser broadcast, 5) multiaccess, 6) interference, and 7) large scale heterogeneous cognitive networks, which may include different combinations of various channel types. Although such a structural review that is channel type and scenario-dependent might ease the review of papers, it unfortunately does not clearly classify and identify in a generic conceptual manner the underlying transmission strategies that are responsible for providing secrecy against eavesdropping in any considered scenario (i.e., scenario-independent).

Moreover, the applications of PLS to some of the emerging wireless systems and technologies such as visible light communication (VLC), body area network (BAN), power line communication (PLC), radio frequency identification (RFID), Internet of things (IoT), device-to-device (D2D), vehicular ad hoc network (VANET), smart grid, ultra-wide-band (UWB), unmanned aerial vehicle (UAV), mm-Wave, cognitive radio, index modulation, and new multiple accessing schemes like non-orthogonal multiple access (NOMA) have been intensifying within the last few years. Thus, it is very significant and worthy to review the most recent state of the art on these important emerging systems that are already being adopted in practice, not only to make the community aware of the research studies that have been conducted in each domain, but also to facilitate understanding the specific requirements imposed on PLS techniques when being applied and adopted in these domains alongside manifesting new research opportunities and directions.

Contribution: Motivated by these observations, in this paper, we first focus our attention on establishing and structuring a unique and unified taxonomy framework that can classify and fit all the existing physical layer security techniques proposed in the literature under one big comprehensive umbrella in a very conceptual, expandable, and easily understandable way. This framework is anticipated to help researchers, engineers, cyber-security practitioners, system designers, students, and interested public from both industry and government sectors in clearly grasping the big picture of physical layer security. Particularly, this framework enables new researchers in this field to easily and quickly catch up with the state of the art, realize the kernel concept behind the enabling security techniques, their advantages and disadvantages, the used secrecy metrics and notions, and how to develop new ones based on the requirements of the applications and services that are targeted to be secured[3].

Besides, it clearly states the learned lessons, remarks, merits, and demerits of the various introduced security methods in the literature so that security designers can know what kind of techniques is more suitable to be used in a certain scenario under specific constraints and requirements. Additionally, with the help of the proposed framework, researchers can solidify their efforts on trying to maximize and maintain the merits of each security technique, while minimizing or even fully overcoming its demerits and drawbacks.

The second exciting part of this survey is the comprehensive discussion and review of the recent applications of PLS to many of the emerging communication systems such as VLC, BAN, PLC, RFID, IoT, D2D, VANET, UWB, UAV, NOMA, mm-Wave, smart grid, cognitive radio, and index modulation-based systems. This inclusive review sheds the light on the implications of employing PLS concepts to these systems and how security designs may require to be deliberately modified according to new requirements and constraints determined by the characteristics of such systems.

Organization: The organizational structure of this paper proceeds as follows. Section II explains the generic system model and main preliminaries of the considered eavesdropping PLS problem. Section III presents and categorizes the secrecy notions and metrics used in PLS to characterize and quantify secrecy performance. Section IV explains and classifies the techniques related to the approach of SNR-based PLS into three major categories: First, secrecy channel codes-based schemes; second, security techniques based on channel adaptation; third, schemes based on injecting intentionally well-designed interfering (noise/jamming) signals alongside the transmitted information signals. The second approach, which is associated with the mechanisms of extracting secret sequences (keys) from the shared channel, is classified into two main categories based on which layer the secret sequence

[3] Note that since this survey is intended to be exclusively devoted to comprehensively review the state of the art **techniques** of physical layer security alongside their classifications and applications, the review of information theory and performance analysis related studies is kept at minimal (i.e., these kind of studies are reviewed briefly wherever is needed in this survey to support the concept and features of the discussed techniques).

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2018.2878035, IEEE Communications Surveys & Tutorials

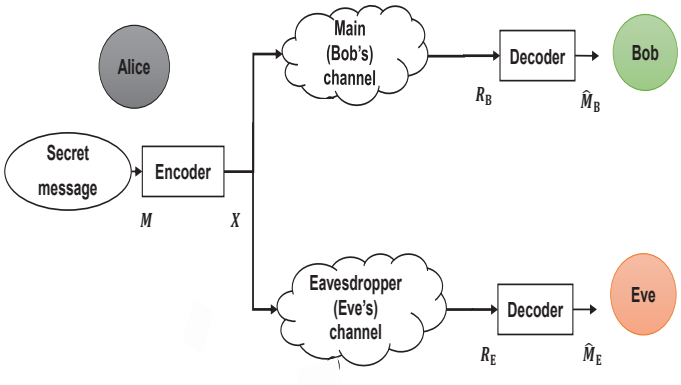

Fig. 1. Generic system model of physical layer security related to eavesdropping problem, in which Alice tries to communicate confidentially with Bob without allowing Eve to get any useful information from the ongoing communication between the legitimate parties (Alice and Bob).

obtained by channel quantization is applied on.

The enabling security techniques pertaining to each one of these categories are divided into three main signal domains: time, frequency and space. For each one of these domains, several examples are given and illustrated along with the review of most recent security advances in each domain. Section V exhibits and reviews the applications of PLS to emerging areas like VLC, BAN, PLC, IoT, smart grid, mm-Wave, cognitive radio, vehicular, UAV, UWB, D2D, RFID, and 5G systems including secure index modulation waveforms and NOMA-based security designs. Section VI offers recommendation and future research direction, followed by a conclusion drawn in Section VII.

II. System Model and Preliminaries

In the generic model of physical layer security problem, we usually have three main communication entities (nodes) as depicted in Fig.1. The first node is basically the legitimate transmitter node, and is referred to as Alice. The second node is the legitimate receiver node, and is referred to as Bob, while the third node, named as Eve, is the malicious eavesdropper node. In this setup, Alice aims at sending secret data content and communicating confidentially with Bob in the presence of Eve that tries to intercept the ongoing communication between the legitimate parties (Alice and Bob). In other words, Eve's target is to decode and obtain the secret data content from her own observations of the received signals.

Accordingly, the goal of Alice is to device and use a transmission technique or method that can deliver the secret data messages intact to Bob, while making sure that Eve is kept ignorant and unable to decode the transmitted secret messages. To achieve secrecy in such scenario, PLS techniques are properly designed via exploiting the channel characteristics including noise, fading, interference, dispersion, diversity, etc., along with the transceiver architecture including synchronization, estimation, hardware impairments, etc., in order to make the data transmission in favor of Alice only, and thus overcoming the eavesdropping problem.

As presented in Fig.1, the confidential information message, M, is encoded into X of length n, and then sent through a wireless channel. The received signals at Bob and Eve are indicated by R_B and R_E, respectively. The entropy of the source information is given by $H(M)$, whereas the residual uncertainty (conditional entropy) for the eavesdropper's observation is denoted by $H(M|R_E)$. Now, based on the scenario and environment under consideration, the availability of channel state information (CSI) at the communication parties varies from complete to partial to even zero knowledge. However, in a practical wireless system, all communication parties can acquire some information about the channel between the transmitter and themselves.

Moreover, Alice is usually assumed to know the CSI of the legitimate receiver by the means of exploiting the reciprocity of the channel in a time division duplexing (TDD) system or by receiving CSI feedback from Bob in a frequency division duplexing (FDD) system. Furthermore, in spite of the fact that Alice has to practically be assumed to have no knowledge about Eve's channel as she is usually passive (i.e., not communicating with the other nodes in the systems, just listening); one can find in the literature that Alice is sometimes assumed to know Eve's channel [25] [26] [27]. This is justified by the fact that Eve can be considered a licensed user who has legal access to the network, but has a bad intention in eavesdropping the communication of other users in the network.

It is also worth to mention the reality that Eve's and Bob's channels are usually assumed to be independent of each other due to the spatial de-correlation property of the wireless channel response (i.e., channels de-correlate and become independent from each others if they are half wavelength apart from each other). However, when the channel is not rich scattering and Eve is located in a close proximity to Bob, then both channels (i.e., Alice-to-Bob and Alice-to-Eve) will be very similar and correlated with each other, and thus Eve can be considered to know Bob's channel in this special case.

III. Secrecy Notions and Performance Metrics

A. Secrecy Notions

In the literature of PLS, there are several common secrecy notions, which are frequently used by researchers as design criteria intended to describe the level of security that a certain scheme or method can provide. In fact, there has been a controversial debate about the exact interpretation of some of these notions such as perfect secrecy, strong secrecy and weak secrecy [28]. Shannon-based works define perfect secrecy to be exactly equal to the legitimate receiver capacity (main channel capacity) when Eve's channel capacity (wiretap capacity) exactly equals zero, i.e., zero information leakage to Eve; for any code length. This definition is modified when the code length tends to infinity, and this results in what is called strong secrecy when the code length is sufficiently long enough.

On the other hand, Wyner-based works considered secrecy to be perfect if and only if the secrecy capacity has a positive value with a certain probability, no matter how much small this value might be and regardless of Eve's capacity

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2018.2878035, IEEE Communications Surveys & Tutorials

Secrecy Notions	Conceptual Definition	Mathematical Definition
Perfect secrecy	The mutual information leakage to Eve must be zero regardless of its processing power and computational capabilities. This notion serves as the most stringent secrecy measure as it ensures almost unity decoding error probability if the entropy of the message is the same as that of the key.	$I\left(M;R_E\right)=0,$ $H(M)=H(M\mid R_E).$
Ideal secrecy	The asymptotic conditional entropy of both the message and the key does not go to zero as the codeword length n goes to infinity. This means that an encryption algorithm is ideally secure if no matter how much of cipher text is intercepted by Eve, there is no unique solution of the plaintext but many solutions of comparable probability.	$\lim_{n\to\infty} H(M\mid R_E)\neq 0,$ $\lim_{n\to\infty} H(K\mid R_E)\neq 0.$
Weak secrecy	The asymptotic mutual information rate goes to zero as the codeword length n goes to infinity. Thus, this notion does not strictly force mutual information leakage to be zero on each channel use, but rather on average.	$\lim_{n\to\infty}\frac{1}{n} I(M;R_E)=0\,.$
Strong secrecy	The asymptotic mutual information goes to zero as the codeword length n goes to infinity. Thus, this notion forces mutual information leakage to be zero on each channel use, but not on average as in weak secrecy	$\lim_{n\to\infty} I(M;R_E)=0.$
Semantic secrecy	It means that it is asymptotically impossible to estimate any function of the message better than to randomly guess it without knowing or considering Eve's observations and over all message distributions.	$\lim_{n\to\infty}\max_{pm} I(M;R_E)=0.$
Distinguishing secrecy	It means that the channel output observations are asymptotically indistinguishable for different input information messages. This achieves strong secrecy over all message distributions.	$\lim_{n\to\infty}\max_{m,m'} \mathbb{V}(p_{R_E\mid M=m}, p_{R_E\mid M=m'})=0,$ $\mathbb{V}(p_{\mathrm{X}},p_{\mathrm{Y}})\triangleq\int_{\mathbb{R}^n}(\mid p_{\mathrm{X}}(\mathbf{x})-p_{\mathrm{Y}}(\mathbf{x})\mid)d\mathbf{x}.$

TABLE I
SECRECY NOTIONS: MEANING AND MATHEMATICAL DEFINITION.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2018.2878035, IEEE Communications Surveys & Tutorials

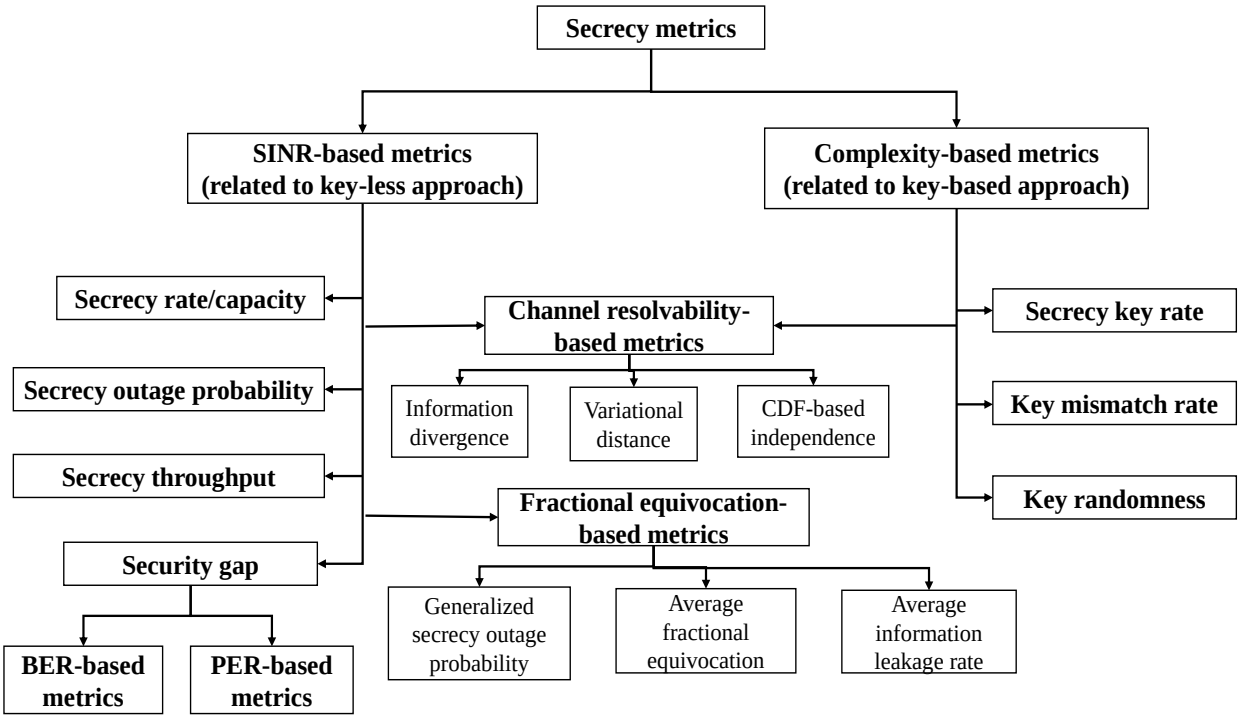

Fig. 2. Classification of the common secrecy performance metrics used to evaluate the security performance of wireless schemes and techniques.

or the amount of information that leaks to Eve. Thus, this definition results in what is called weak secrecy, in which there exists a rate (usually small and affected by SNR) at which perfect communication can be achieved. Besides the notions of perfect, strong, and weak secrecy; there are also other notions which are used to describe different secrecy levels such as ideal secrecy, semantic secrecy, and distinguishing secrecy.

Table I briefly explains and summarizes the conceptual meaning as well as the mathematical definition of the most popularly used secrecy notions in the literature. In the table, $I(\ ;\ )$ means the mutual information, $H(\ )$ is the information entropy, $H(\ |\ )$ is the conditional information entropy, K is the secret key sequence, pm is the probability distribution of the message; m, m' are defined to be different input messages and $\mathbb{V}(p_{\mathsf{X}}, p_{\mathsf{Y}})$ is the statistical or variational distance, which can be given as

$$\mathbb{V}(p_{\mathsf{X}}, p_{\mathsf{Y}}) \triangleq \int_{\mathbb{R}^n} |p_{\mathsf{X}}(\mathbf{x}) - p_{\mathsf{Y}}(\mathbf{x})| d\mathbf{x}. \tag{1}$$

For more information on the dependencies related to secrecy notions, we refer the reader to [29].

B. Secrecy Performance Metrics

One of the most important steps that has to be performed after designing any security scheme or technique is to properly evaluate and quantify its secrecy performance using a suitable metric. The performance evaluation must reflect how much secrecy the proposed scheme or method can provide. Without loss of generality, the secrecy metrics used in the literature can be classified into two major classes as exhibited in Fig.2. The first class, which is associated with key-less-based PLS techniques, is named as SINR-based metric; whereas the second class, which is associated with key-based PLS methods, is called complexity-based metric.

The SINR-based metrics include secrecy rate or secrecy capacity, secrecy outage probability, secrecy throughput, fractional-equivocation-based metrics, BER-based and PER-based metrics. Secrecy channel capacity [2] is the most commonly used metric defined as the difference between the legitimate and eavesdropper's channel capacities. More precisely, it defines the maximum secrecy rate at which the message is recovered reliably at Bob while keeping it useless and unrecoverable at Eve. This metric is later extended by researchers to outage secrecy and outage secrecy rate probability [30] in order to better measure the resulting secrecy in fading environments. Although secrecy capacity metric is very popularly used in the literature by information theoreticians, it does not necessarily reflect the actual obtained secrecy in practical transceiver designs with different communication services, but rather shows the achievable bounds considering the random channel behavior. However, to get the actual practical secrecy performance, error probability rate difference between Eve and Bob has been adopted by the signal processing and system design communities. An example on this is bit error rate (BER) [31] and packet error rate (PER) [32], which can directly be linked with secure throughput [33] and thus with

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2018.2878035, IEEE Communications Surveys & Tutorials

secrecy channel capacity.

Despite the usefulness of traditional secrecy outage probability in evaluating and characterizing the security performance of wireless channels, it has three main demerits. First, it lacks the ability to quantitatively characterize the amount of information leakage to the eavesdroppers when outage secrecy happens. Second, it cannot provide any insights on the eavesdropper's capability in successfully decoding the confidential messages. Third, it cannot be linked with the Quality of Service (QoS) requirements of different applications and services. Motivated by these facts, authors in [34] proposed three new metrics based on the distribution of fractional equivocation (partial secrecy) given by ($\Delta = \frac{H(M|R_E)}{H(M)}$) [35], which can be obtained from channel gains distributions. These metrics include generalized secrecy outage probability, average information leakage rate, and average fractional equivocation.

The second class of metrics (i.e., complexity-based metric), is mainly used for key-based methods. This metric is adopted for this kind of methods because an eavesdropper may become eventually able to guess the key (if it has sufficient time and powerful processing capabilities) using exhaustive search process or what is commonly called as brute-force attack[4]. In this approach [22], designers are mostly interested in measuring the length of the key extracted from the channel since the longer the key is the better the secrecy level will be as it would be harder for Eve to crack the key. Note that keys are desired to be long enough with high entropy and uniform distribution. Besides, the key disagreement (mismatch) probability between the transmitter and receiver is a very important metric to be measured as it reflects whether the proposed method will degrade the legitimate receiver performance or not.

It should be noted from the classification figure of secrecy metrics (i.e., Fig.2) that there is a third class of metrics which can be used for both types of secrecy i.e., for SINR-based metrics and complexity-based metrics.

One important point we should emphasize here is that error rate probability at eavesdroppers does not fulfill any of the secrecy requirements in this case, thus it is not suitable to be used in key-based approach. Moreover, channel resolvability-based metrics [36] including information divergence, variational distance, and CDF-based independence between the transmitted message and its observation at Eve can be used to measure the secrecy of key-based methods as well as keyless methods.

For more details on learning how to accurately measure and calculate these metrics alongside their mathematical definitions and the differences between them, we refer the reader to our related tutorial paper available in [29].

[4]Brute-force attack is a trial and error technique adopted by specialized software programs to decrypt secure data such as passwords or keys, through using exhaustive search process. A brute-force cracking method tries all possible combinations of legitimate symbols or characters in a sequence until it find the correct solution. Brute-forcing is considered to be a very effective, yet time-consuming and complex approach. Besides, it is worth noting that methods using symmetric keys of sufficient length and good properties have the potential to become post-quantum-computing safe

IV. Security Techniques Classifications

In Fig.3 and Fig.4, we explicitly draw and show from a high level perspective of the big picture of PLS, the conceptual classification structure of PLS approaches divided into SINR-based and complexity-based ones. For each approach, we mention the kernel enabling techniques along with the main domains corresponding to each security technique including time, frequency and space. In this section, we go over these general enabling techniques one by one, explain their concepts, advantages, disadvantages, review examples from the literature on each technique, and finish each subsection with stating the lessons learned from each domain.

A. Secure Channel Coding Design [I]

Error control codes constitute a substantial part in establishing reliable secure systems when Eve's channel is worse (i.e., experience more degradation) than that of Bob on average. In fact, after the foundations of information-theoretic security had been established, many researchers focused their efforts on the development and design of practical secrecy-achieving channel codes. Wyner and other researchers had proven the existence of randomized channel codes that ensure both reliability and confidentiality as the block length tends to infinity. Here, we summarize some of the main works performed in this area of research. The first practical secrecy code design was proposed in [37] using Coset (syndrome) coding.

In [38], authors studied from an information-theoretic perspective the fundamental limits and coding methods of wiretap channels. They showed how the capacity achieving codes can be exploited to reach the secrecy capacity of any wiretap channel by adopting codes that are capable of achieving the capacity of Eve's channel. Specifically, they stated that it is feasible and possible to design linear-time decodable secrecy codes by using **low-density parity-check (LDPC) codes** that are capable of achieving secrecy. Furthermore, in the same study, the authors used nested sparse graph-based LDPC codes to achieve the secrecy capacity when Bob's channel is noiseless, whereas Eve's channel is binary erasure channel (BEC).

In [39], authors proposed a secure nested code structure with a new achievable secrecy rates, which improves upon the previously reported result by [38] when the main channel is noiseless and the eavesdropper channel is a general binary-input symmetric-output memoryless channel. In [40], researchers investigated the performance of punctured LDPC codes under maximum-likelihood (ML) decoding under the same scenario [38], [39]. In particular, it was proven that capacity-achieving codes of any memoryless binary-input output-symmetric (MBIOS) channel and for any rate under ML decoding can be constructed by puncturing some original LDPC codes with small enough rate.

For Gaussian wiretap channel, [41] presented a practical coding scheme based on LDPC coding scheme, which is encodable in linear time, applicable at finite block lengths, and can be combined with existing cryptographic schemes to provide improved data security by taking advantage of the statistical nature of communication channels. In [42], authors

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2018.2878035, IEEE Communications Surveys & Tutorials

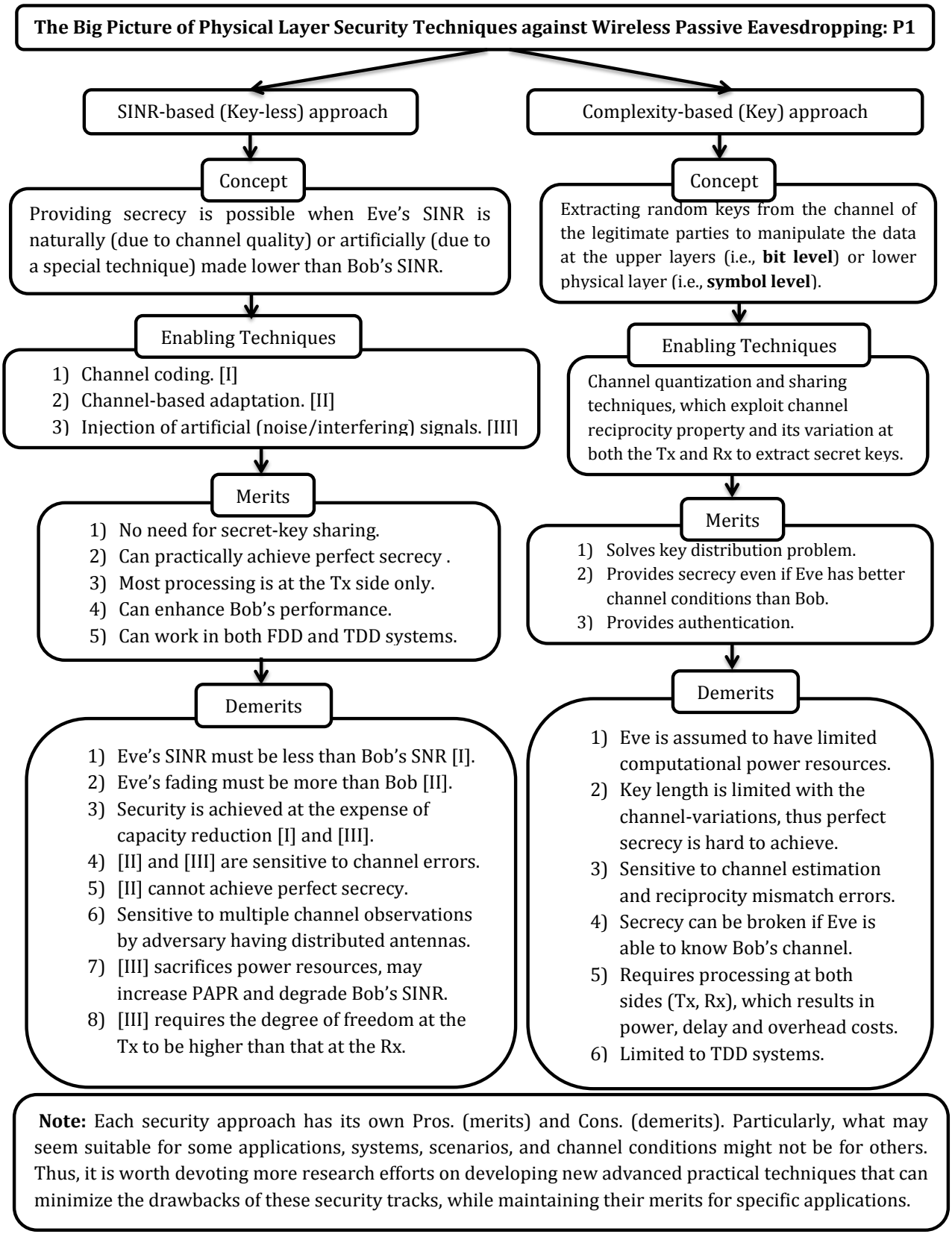

Fig. 3. The big picture of the classification structure (including concepts, merits, and demerits) of physical layer security techniques against wireless passive eavesdropping: Part one (P1).

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2018.2878035, IEEE Communications Surveys & Tutorials

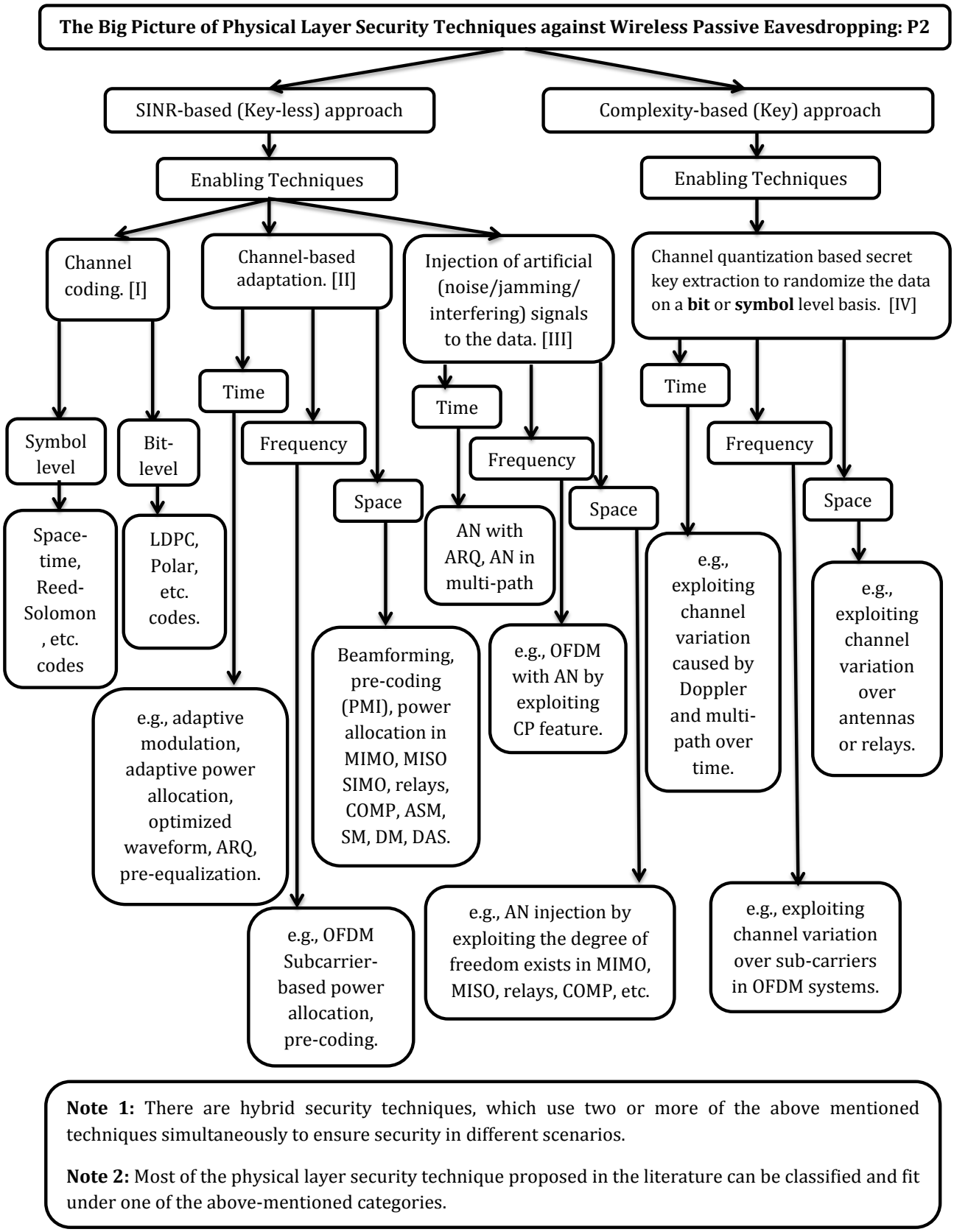

Fig. 4. The big picture of the classification structure (including examples in the three main signal domains: time, frequency, and space) of physical layer security techniques against wireless passive eavesdropping: Part two (P2).

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2018.2878035, IEEE Communications Surveys & Tutorials

assessed the behavior of some LDPC code design techniques over the AWGN wiretap channel, in terms of security gap. In [43], the authors studied the application of a special type of LDPC codes based on serially concatenated low-density generator matrix to the Gaussian wiretap channel. In [44], the equivocation rate of Eve's channel is exploited as an optimization criteria for designing an algorithm in the finite codeword length regime. By using this algorithm, irregular LDPC codes with smaller codeword lengths are constructed that can approach the ultimate performance limits.

A brief summary of some of the key contributions related to secure LDPC codes is provided in Table II.

Recently, **polar codes**, which are known as capacity achieving codes, are proposed to be used as secrecy capacity achieving codes too. In [45], authors used polar codes to construct a coding scheme that achieves the secrecy capacity for a wide range of wiretap channels. Their scheme works for any instantiation of the wiretap channel model, as long as both main and wire-tap channels are symmetric and binary-input, and wire-tap channel is degraded with respect to the main channel. Moreover, they clarified how to modify their construction in order to provide strong security, in the sense defined by Maurer. In [46], it was shown that polar codes can achieve nonzero perfect secrecy rates for the binary-input degraded wiretap channel with low encoding-decoding complexity. Also, in the special case of having symmetric channels for both Bob and Eve, this coding technique achieves the secrecy capacity. This approach was also extended to the multiple-access channel with a degraded eavesdropper where a nontrivial achievable secrecy region is established. In [47], a new multi-block polar coding scheme is introduced on top of [45] to resolve the difficulty in providing both strong security and reliability using polar codes, which occurs due to the existence of a small number of bit-channels that are both unreliable and unsecure.

In [48], authors proposed a concatenated coding scheme based on polar codes and LDPC codes for the AWGN wiretap channel. They also presented a transmission scheme using rate compatible Polar-LDPC codes to adapt for different dynamic environments. In [49], a feedback-based secrecy coding scheme using polar code over wiretap channels was proposed, where authors' results show that the proposed scheme using polar code can transmit confidential messages reliably and securely. In [50], authors proposed an alternative approach to the traditional way of generating secret keys, based on polar codes that jointly deals with reliability and secrecy. In [51], a low-complexity and secrecy capacity achieving polar coding scheme was developed for the discrete memoryless wiretap channel. The scheme extends previous work by using a nearly optimal amount of uniform randomness in the stochastic encoder, and avoiding assumptions regarding the symmetry or degraded nature of the channels. In [52], polar codes are developed to relax the symmetric and degraded constraints. In addition, the coding scheme is also extended to the interference channel with confidential message (IC-CM), broadcast channel with confidential message (BC-CM), and to the multiple access wiretap channel (MA-WC). Besides, a secrecy capacity achieving coding scheme is introduced in [53] for general wiretap channel based on polar codes (not necessarily symmetric or degraded). In [54], the authors proposed an interesting security technique for the wiretap channel based on polar codes and artificial noise (AN). In this technique, the channel quality advantage of Bob over over that of Eve is not assumed. In the first step, upper and lower bounds on the symmetric capacity of the polarized bit-channels are derived that depends on the SNR of each use of physical channel. Based on these bounds they prove that there is an existence of bit channels that are hostile to signal reception of the wiretap channel but beneficial to main channels. Moreover, they also introduce a method to achieve these bit channels based on injecting AN and also prove the security of proposed AN method theoretically. Furthermore, they also introduce two power allocation schemes for AN.

A short summary of some of the main contributions related to secure polar codes is made in Table III.

Besides designing security schemes based on LDPC and polar codes, there are other secrecy schemes based on lattice codes such as the works reported in [55], [56] and [57]. In addition, the application of the practical convolutional and turbo codes to Gaussian wiretap channel using randomized encoding approach and based on using security gap metric has recently been studied in [58].

Lesson 1: Most of the security codes surveyed in the aforementioned studies are usually designed based on the criterion of weak or strong secrecy notion which generally assumes infinite block length, making it less practical for multimedia communication services (such as voice, video, etc.) where the block length is finite due to having constraints on the delay and throughput of these type of services that also do not usually require perfectly zero block error probability. Particularity, the research community should pay more attention to the fact that we need to design practical security codes for the cases where the block length is finite[5] (does not go to infinity [63]), and secrecy rate does not necessary require to be exactly equal to the main channel capacity where there is zero information leakage to Eve. This is due to the fact that Eve cannot practically benefit from a service that does not meet or comply with its minimal quality requirements. Moreover, the design of practical security codes that not only can achieve the secrecy capacity limit of finite block length, but also comply with the practical constrains including delay, throughput and complexity of some of the emerging communication services in 5G and beyond scenarios such as URRLC and mMTC remains a challenging task to achieve. Besides, to the best of authors' knowledge, designing generic secrecy codes without considering any information knowledge on the channel of the eavesdropper (which is a very practical scenario) is also not yet clear or known thus far in the literature. Therefore, novel coding techniques are indeed needed to address the above challenges.

[5]Note that there are a few primarily recent theoretical results related to the fundamental limits of secrecy coding for finite block length as can be found in [59]–[62].

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2018.2878035, IEEE Communications Surveys & Tutorials

TABLE II
CHANNEL CODING FOR PHYSICAL LAYER SECURITY (LDPC CODES)

Authors	Year	Contributions and Concepts
A. Thangaraj *et al.* [38]	2007	Nested sparse graph-based LDPC codes are used to achieve the secrecy capacity when Bob's channel is noiseless, whereas Eve's channel is binary erasure channel (BEC).
R. Liu *et al.* [39]	2007	A secure nested LDPC code structure with a new achievable secrecy rates is presented whose performance is better than the previously reported result by [38] when the main channel is noiseless and the eavesdropper channel is general binary-input symmetric-output memoryless channel.
C.-H. Hsu *et al.* [40]	2008	It is proven that capacity-achieving codes of any memoryless binary-input output-symmetric channel can be constructed under ML decoding by puncturing some original LDPC codes with small enough rate considering same scenario as [38], [39].
D. Klinc *et al.* [41]	2011	A practical coding scheme based on LDPC for Gaussian wiretap channel is presented which is encodable in linear time, applicable at finite block lengths, and can be combined with existing cryptographic schemes to provide improved data security.
N. Maturo *et al.* [42]	2013	The behavior of some LDPC code design techniques is addressed over the AWGN wiretap channel in terms of security gap.
Nooraiepour *et al.* [43]	2018	The application of a special type of LDPC codes based on serially concatenated low-density generator matrix to the Gaussian wiretap channel is investigated.

TABLE III
CHANNEL CODING FOR PHYSICAL LAYER SECURITY (POLAR CODES)

Authors	Year	Contributions and Concepts
H. Mahdavifar *et al.* [45]	2011	Polar codes are used to construct a coding scheme that achieves the secrecy capacity for a wide range of wiretap channels under the condition that both main and wire-tap channels are symmetric and binary-input, and wire-tap channel is degraded with respect to the main channel.
O. Koyluoglu *et al.* [46]	2012	It is demonstrated that the polar codes can achieve non-zero perfect secrecy rates for the binary-input degraded wiretap channel with low encoding-decoding complexity.
E. Sasoglu *et al.* [47]	2013	A new multi-block polar coding scheme is introduced on top of [45] to resolve the difficulty in providing both strong security and reliability using polar codes.
Y. Zhang *et al.* [48]	2014	A concatenated coding scheme based on polar codes and LDPC codes for the AWGN wiretap channel is proposed. Moreover, a transmission scheme using rate compatible Polar-LDPC codes to adapt for different dynamic environments is also presented.
L. Song *et al.* [49]	2014	A feedback-based secrecy coding scheme using polar code over wiretap channels is proposed.
R. A. Chou *et al.* [50]	2015	An alternative approach to the traditional way of generating secret keys is proposed based on polar codes that jointly deals with reliability and secrecy.
R. A. Chou *et al.* [51]	2015	A low-complexity and secrecy capacity achieving polar coding scheme is developed for the discrete memoryless wiretap channel with nearly optimal amount of uniform randomness in the stochastic encoder.

B. Channel-Based Adaptation Transmission [II]

Concept: The starting point of this direction was first inspired and initiated (from basic information-theoretic perspective) by Bloch *et al.* [30], Liang *et al.* [64], and Gopala *et al.* [65], concurrently (in the same year) but independently. In these works, it was proven that non-zero secrecy rate can be achieved in a wireless fading environment even when Eve's SNR is equal to or higher than Bob's one on average since there will always be times where Bob's instantaneous channel condition is better than Eve's one because of the independent fading phenomena between Alice-to-Bob and Alice-to-Eve channels. Thus, by designing an optimal or adaptive transmission scheme, perfect secure communication can be achieved at a certain rate.

Without loss of generality, this security technique takes its effective role when the transmitter optimizes or adapts its transmission parameters according to the wireless fading channel conditions, location, and requirements of the legitimate receiver. Since the transmitted signal is set to be optimal for Bob's channel, but not anybody else. This essentially results in a better SNR at Bob compared to Eve, who experiences a different channel from Bob. Thus, Bob in this case does not need to perform any extra processing to decode his data. The basic block diagram of channel-based transmission adaptation for PLS is presented in Fig. 5. Adaptive transmission based on legitimate receiver's CSI requires full or partial channel knowledge at the transmitter which can be obtained by using reference sounding signals (used mostly in time division duplex (TDD) systems) or by sending explicit frequent CSI feedback updates (used mostly in frequency division duplex (FDD) systems) about the conditions and status of the receiver's channel so that the transmitter can adjust (adapt/optimize) its transmission parameters accordingly.

Beside the feedback related to CSI knowledge at Alice, there are other important feedbacks, which can be useful for security such as ACK and NACK messages in ARQ process, pre-coding matrix indicator (PMI) and rank indicator (RI) in MISO and MIMO systems, received signal strength indicator (RSSI), type of application used at user's side, etc. This kind of signaling information (i.e., feedback or partial/full

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2018.2878035, IEEE Communications Surveys & Tutorials

TABLE IV
CHANNEL-BASED ADAPTATION TRANSMISSION (TIME DOMAIN)

Authors	Year	Contributions and Concepts
H. Khodakarami *et al.* [66]	2012	A secure link adaptation framework, which exploits the spontaneous fluctuations of fading channels for PLS against eavesdropping, is proposed.
M. Taki *et al.* [67]	2013	A discrete rate adaptation through adaptive modulation and coding based on SNR of the links to provide secure communication systems is proposed.
M. Li *et al.* [26]	2013	A novel waveform is designed by finding the optimal waveform energy that maximizes SINR at the legitimate receiver and minimizes SINR at Eve.
S. Tomasin *et al.* [68]	2014	Secrecy features added to HARQ protocol by which it becomes a secure HARQ (S-HARQ) scheme.
S. Kundu *et al.* [69]	2014	The optimal power allocation sequence over the H-ARQ rounds is proposed that maximizes the outage probability of eavesdroppers.
Z. Zhong *et al.* [70]	2014	A channel matched scheme of LDPC based secrecy coding for the fast fading channel is designed in which secret message bits are first interleaved based on the fading coefficients of Bob's channel to conceal positions, and then replaced with random dummy bits to hide information.
J. M. Hamamreh *et al.* [32]	2016	An ARQ protocol with maximal ratio combination (MRC) based security scheme is proposed. Moreover, adaptive modulation was also proposed to be used along with ARQ and MRC.
J. M. Hamamreh *et al.* [71]	2017	A secure waveform is proposed in which orthogonal transform basis functions are extracted from the channel to modulate and demodulate the data symbols securely.
H. M. Furqan *et al.* [72]	2017	A security scheme based on channel shortening is proposed in which the equalizer is designed in such a way that the length of the effective channel impulse response is made less than the CP at Bob only.

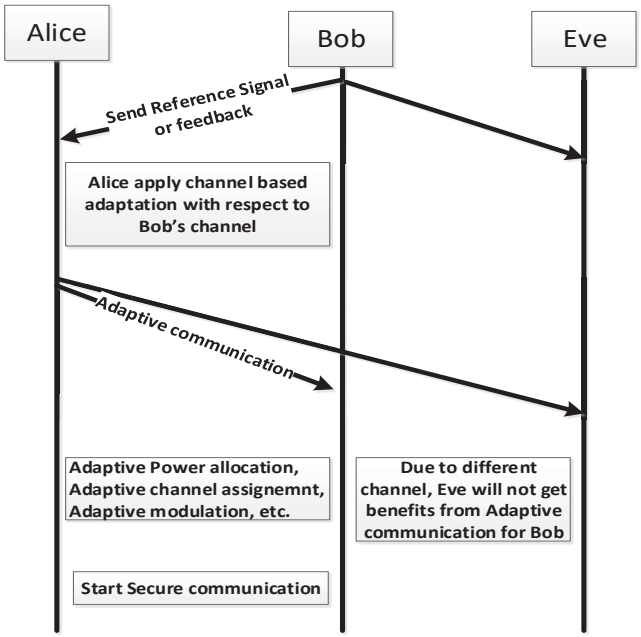

Fig. 5. Basic procedure of the concept for channel-based adaptive transmission for providing security against eavesdropping.

CSI) enables the transmitter to perform adaptive coding and modulation, optimal power allocation, adaptive scheduling and resource allocation, adaptive waveforms and pulse shaping, partial pre-equalization, pre-coding, antenna selection, pre-filtering, and/or adaptive interleaving etc., to just meet the requirements of the legitimate user, while making the signal look random (unoptimized) with respect to the eavesdropper.

Merits: In fact, this kind of security techniques not only enhances physical security, but also saves power, fosters efficiency, and increases Bob's reliability. Additionally, it is suitable to be deployed in TDD, FDD, or hybrid division duplex systems, where both FDD and TDD are utilized together. More importantly, even if Eve knows the feedback, she cannot benefit much from it and will not reach the performance of Bob, and there will always be a specific design at which secrecy can be achieved. Also, this approach does not usually impose the receiver to perform extra processing, making it suitable for low-complexity devices such as sensors and actuators in IoT systems.

Demerits: Although this approach frees and releases the receiver from any extra processing, which is highly desirable in future technologies and Internet of Things (IoT) devices, it still cannot achieve perfect secrecy by its own and there will mostly be an information leakage to Eve. As a final note on this approach, it is very important to realize that the existence of cooperative eavesdroppers with multiple signal observations may lead to zero secrecy capacity. Thus, integrating this approach with other security approaches (that will be discussed later) may become inevitable to avoid such demerits.

In the following, we review some of the major works, techniques, and studies related to this subject according to the specific type of signal domain (i.e., time, frequency, or space) that the method is exploiting.

1) Time Domain Security: In time domain, the information-carrying signal is transmitted and received in time domain over one carrier frequency using a single antenna. In fact, physical layer security has become very popular after introducing the importance of fading channels for providing secrecy where non-degraded eavesdropping channel is assumed (more close to practical scenarios). The related-information theoretical works in [30], [64], [65], [73]–[77] assure that one can design an adaptive scheme that can attain perfect secrecy (in the weak sense) at a certain rate by adopting the transmission to the channel conditions of the legitimate user, assuming that the channel knowledge can be acquired at the transmitter by using either channel sounding techniques in TDD systems

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2018.2878035, IEEE Communications Surveys & Tutorials

or feedback in FDD systems. The authors of [78] studied (from an information-theoretic point of view) hybrid automatic retransmission request (HARQ) protocol, which provides time diversity, in a block-fading wire-tap channel. Authors investigated the secrecy performance and error of repetition time diversity (RTD) or what is also called in the literature as chase-combing (CC), and incremental redundancy (INR) protocols based on Wyner code sequences. They illustrated that there exists a rate-compatible Wyner codes that can achieve a secure HARQ protocol.

In [85], authors showed that the use of HARQ protocol with authentication allows achieving a sufficient level of security. Later, the coding scheme proposed in [78] was questioned by [86], where it is stated that the coding scheme of [78] is based on a mother code that contains a unique secrecy parameter, which causes a strong drawback for this secure HARQ protocol because it must be adapted to all possible retransmissions even if they do not occur, resulting in a huge throughput degradation (i.e., not practical for some services). Therefore, [86] proposed a new coding scheme called SARA-code, which provides secrecy adaptation and rate adaptation in HARQ protocol. In [87], [88], authors showed, via analyzing the achievable secrecy throughput in incremental redundancy secure HARQ protocols over block-fading wiretap channels, how to find the optimal rate-adaptation policies to maximize the secrecy throughput under constraints on outage probabilities.

In [68], authors added secrecy features to HARQ protocol by which it becomes a secure HARQ (S-HARQ) scheme. They also characterized the set of channels for which there exists a sequence of codes that ensure both zero error probability to Bob and zero rate of information leakage to Eve in the limit of infinitely long code-words. This later scheme suffers too much from throughput degradation as the one studied in [78]. In [69], authors found the optimal power allocation sequence over the H-ARQ rounds that maximizes the outage probability of eavesdroppers for any given target outage probability of the intended receiver. In [32], we proposed an ARQ protocol with maximal ratio combination (MRC) based security scheme. We also derived exact the packet error rate (PER) formulas for both Eve and Bob in i.i.d block Rayleigh fading channel. The simulation results showed that the employment of ARQ and MRC provides security gap in the resulting PER performance. Moreover, in order to further enhance the security and to provide quality of service (QoS)-based security at any SNR, adaptive modulation was proposed to be used along with ARQ and MRC. Analytical and simulation results show that there is a significant PER performance gap between Bob and Eve's performances.

Inspired by the theoretical results of secrecy over fading channel, several researchers have proposed effective practical techniques to achieve secret communication. Among these, [66] demonstrated that link adaptation is very advantageous for providing PLS over wireless fading channels. Specifically, a secure link adaptation framework, which exploits the spontaneous fluctuations of fading channels for high-performance communications and PLS against eavesdropping, is proposed. Authors of [67] proposed a discrete rate adaptation through adaptive modulation and coding based on SNR of the links to provide secure communication systems.

A channel matched scheme of LDPC based secrecy coding for the fast fading channel was designed in [70], in which secret message bits are first interleaved based on the fading coefficients of legitimate main channel to conceal positions, and then replaced with random dummy bits to hide information from potential eavesdroppers. Due to the different features of main and eavesdropper's channels, the proposed scheme ensures that the trusted receiver can reconstruct the confidential message, while the eavesdropper almost cannot extract any information. In [89], researchers proposed a new framework for determining the wiretap optimized code rates of single-input-single-output multi antenna eavesdropper wiretap channels when the eavesdropper's channel is not available at the transmitter. Authors of [90] obtained a set of power control schemes under diverse system parameters over wireless fading channel and using statistical security model to provide physical security.

In [26], authors developed a novel waveform design approach to minimize the likelihood that a message transmitted wirelessly between trusted single-antenna nodes is intercepted by an eavesdropper via finding the optimal waveform energy that maximizes SINR at the legitimate receiver and minimizes SINR at the eavesdropper. In [71], [91], we proposed a secure waveform, called orthogonal transform division multiplexing (OTDM) waveform, for 5G and beyond. Particularity, we used orthogonal transform basis functions that are extracted from the channel instead of IFFT and FFT used in OFDM to modulate and demodulate the data symbols securely. The schematic diagram of this scheme is briefly explained in Fig. 6. The proposed design in [71] not only provides security but can also provide reliability gain over OFDM depending on the channel delay profile of the channel.

In [72], we proposed a spectral and power efficient security scheme based on channel shortening. The basic concept was to design channel shortening equalizer and apply it at the transmitter after IFFT process in such a way that the length of the effective channel impulse response is made equal to or less than the cyclic prefix (CP) at Bob, while the length of the effective channel at the illegitimate receiver (Eve) is made greater than CP. Thus, this causes inter-symbol-interference (ISI), loss of orthogonality, and ultimately overall performance degradation to Eve.

A brief summary of some of the key contributions related to adaptation in time domain is provided in Table IV.

2) Frequency Domain Security: In frequency domain, one time slot or block of data symbols is transmitted and received over multiple sub-carrier frequencies using a single antenna. Thus, this scheme is mostly, as the name implies, related to adaptation in multi-carrier systems such as OFDM technology. In this section, we mention and review some of these works. In chapter one of [9], authors studied the secrecy capacity of a system consisting of multiple independent parallel sub-channels such as OFDM. They showed that the extra dimensionality available in such systems eases secret communication and enhances the secrecy capacity. Moreover, they obtained the optimal power allocation strategy for the case when the sub-

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2018.2878035, IEEE Communications Surveys & Tutorials

TABLE V
CHANNEL-BASED ADAPTATION TRANSMISSION (FREQUENCY DOMAIN)

Authors	Year	Contributions and Concepts
E. Guvenkaya *et al.* [79]	2014	Secure communication scheme for frequency selective channels via fade-avoiding sub-channel usage is proposed.
X. Chen *et al.* [80]	2015	A power-efficient joint resource allocation for multiuser wiretap OFDM channels is investigated to enhance the efficiency and security.
M. Yusuf *et al.* [81]	2016	Signal space diversity is exploited to improve the secrecy of OFDM systems by utilizing a channel-based interleaving pattern.
M. Yusuf *et al.* [82]	2016	A scheme that introduces intentional self inter-carrier interference to pre-cancel the carrier offset at only the legitimate user is proposed.
J. M. Hamamreh *et al.* [83]	2017	An efficient, hardware-friendly PLS scheme for OFDM-based systems is presented where channel-based frequency domain pre-coder and post-coder that work like adaptive interleaver and deinterleaver, respectively, are used.
J. M. Hamamreh *et al.* [84]	2017	OFDM with subcarrier index selection along with adaptive interleaving is proposed, where the whole OFDM block is divided into small sub-blocks, each experiencing good and bad subchannels, and only the subcarriers corresponding to the good subchannels are used for data tranmission.

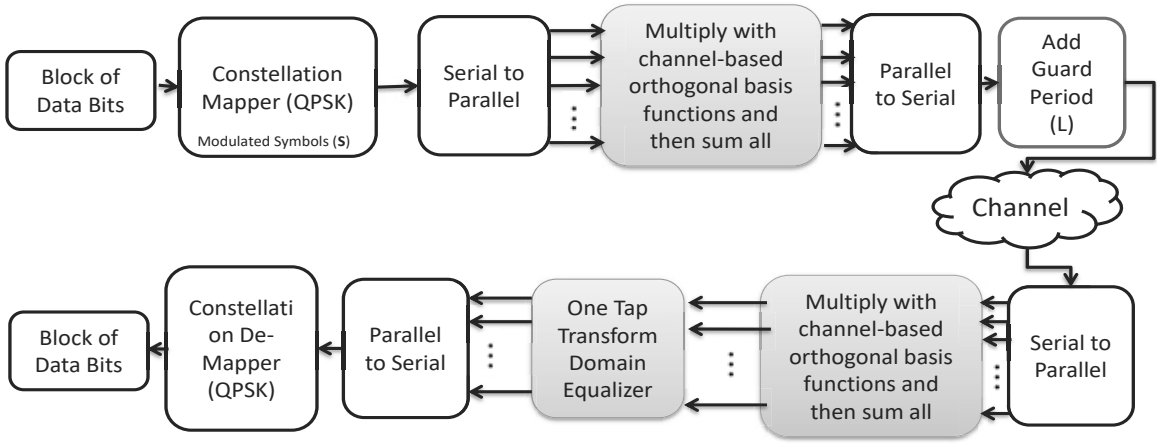

Fig. 6. The transceiver structure of secure orthogonal transform division multiplexing waveform (S-OTDM) proposed in [71], [91] for providing confidentiality against eavesdropping. Note that channel-based transforms are used instead of IFFT and FFT blocks to provide inherently secure modulation and demodulation.

channels are AWGN and the system works under a total power constraint. The obtained optimal power allocation design is similar to the famous water-filling strategy except that the sub-channels are ranked according to the difference between channel gains.

In [92], the achievable rates of information theoretic secrecy by OFDM transmitter/receiver pair were studied and investigated in the existence of Eve who may either use an OFDM design or adopt a more complex receiver design. The authors provided performance evaluation of the achievable secrecy rates of several precoding techniques, such as optimal input using generalized singular value decomposition (GSVD), water-filling and optimal power allocation with independent inputs. Authors also considered the loss in secrecy due to the OFDM transceiver structure, and the information leakage to Eve that uses a much more sophisticated receiver structure.

In [93], two schemes based on resources optimization (power and rates) were considered to achieve security in parallel channels. In one case, the secret message is encoded with a single wiretap code and then split among the sub-channels. In the latter case, the secret message is first split into a number of sub-messages, each separately encoded and transmitted on a different sub-channel. In [79], secure communication in frequency selective channels is achieved via fade-avoiding sub-channel usage, in which adaptive transmission scheme that does not use the faded sub-channels of the legitimate channel for conveying information is considered. Thus, a reduction in the eavesdropper channel capacity, which is proportional to the unused sub-channels, is attained. In [94], the problem of resource allocation for a multiuser OFDMA downlink with eavesdropping was studied, where the optimal power allocation that maximizes the fairness and minimizes the information leakage was obtained.

In [80], a power-efficient joint resource allocation for multiuser wiretap OFDM channels was investigated to enhance the efficiency and security. In [95], authors considered the problem of resource allocation scheme for physical layer security in cooperative OFDM networks using amplify-and-forward (AF) strategy. To maximize the secrecy rate, the joint optimization of power allocation, subcarrier allocation and subcarrier pairing was proposed. In [83], we proposed a hardware-friendly, practical and power efficient physical layer

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2018.2878035, IEEE Communications Surveys & Tutorials

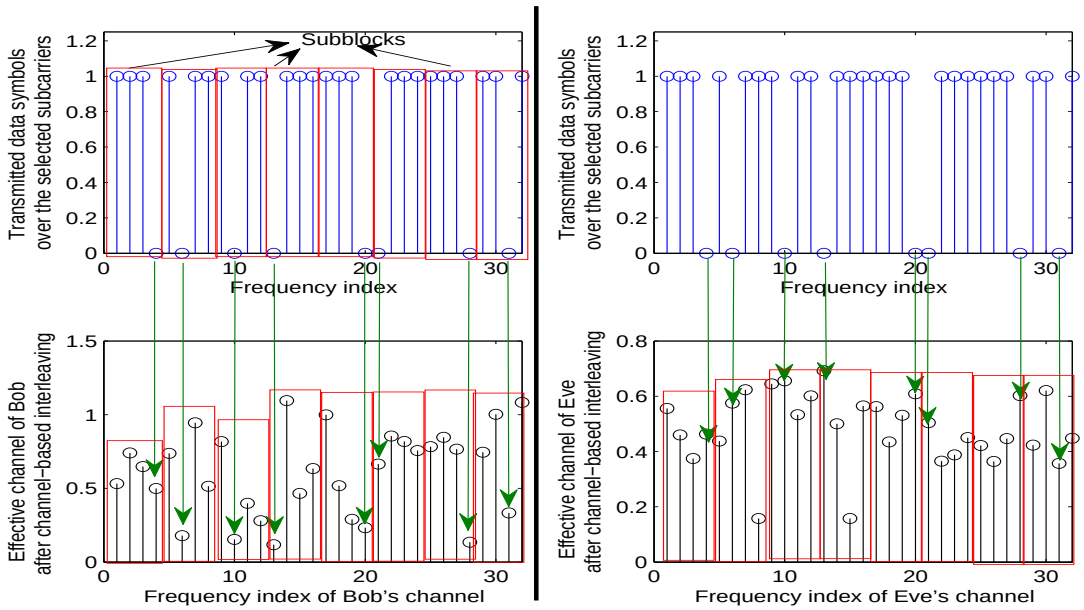

Fig. 7. Subcarrier structure of the OFDM-SIS scheme [84]: In each sub-block, surrounded by red rectangle, the sub-carriers experiencing good sub-channel gains with respect to Bob are used for data transmission, while the rest are nulled. Note that with respect to Eve, the nulled sub-carriers do not usually correspond to the weak (bad) sub-channels.

security design for OFDM based systems by using channel-based frequency domain pre-coder and post-coder. The pre-coder and post-coder are unitary matrices that are designed by decomposing the diagonal matrix of the channel frequency amplitude of the legitimate receiver. The scheme is shown to deliver security as well as providing BER performance improvement when channel coding is used. The provided simulations and USRP hardware testbed implementation results show that the scheme can provide a low complexity, secure, and reliable communication between legitimate parties. In [84], we proposed a scheme, called OFDM with subcarrier index selection (OFDM-SIS) and adaptive interleaving, where the whole OFDM block is divided into small subblocks, each experiencing good and bad subchannels. The scheme performs optimal channel-based selection of the subcarrier indices in each subblock that maximize the signal-to-noise ratio at only the legitimate receiver. It is demonstrated that OFDM-SIS scheme results not only in secrecy performance enhancement but also in reliability improvement to legitimate user only, while saving power, and reducing complexity, making it a very suitable candidate for 5G ultra-reliable low-latency communications (URLLC) service. The schematic diagram of this scheme is briefly illustrated in Fig. 7.

In [81], signal space diversity, which separates the in-phase and quadrature components of the complex modulated symbols and send them over independent uncorrelated fading subchannels, was utilized to improve the secrecy of OFDM systems by utilizing a channel-based interleaving pattern to provide more diversity gain to the legitimate user compared to Eve. In [82], the sensitivity of OFDM to frequency synchronization errors was exploited by a scheme that introduces self inter-carrier interference to pre-cancel the carrier offset at only the legitimate user in order to provide confidentiality against eavesdropping.

A brief summary of some of the key contributions related to adaptation in frequency domain is provided in Table V.

3) Space Domain Security: In space domain, the signal of interest consists of one time slot, one carrier frequency, but several spatial transceiver sources (e.g., antennas). In general, space domain includes multiple input multiple output (MIMO), single input multiple output (SIMO), multiple input single output (MISO), relays, cooperative multi-point (CoMP) systems, distributed antenna system (DAS), and so forth. Providing secrecy via adaptation in space domain is another vital type of security approach that can be realized in practical systems. In this approach, the transmitter adapts and optimizes its different transmission parameters based on the channel characteristics of the legitimate receiver in order to improve the secrecy performance, while preventing eavesdroppers from successfully decoding the data. This can be realized and exemplified by using beamforming, precoding (ZF, MMSE, GSVD, GMD, PMI), full/partial pre-equalization, adaptive power allocation, transmit antenna selection, interference alignment, cooperation and relay selection, etc. The information theoretic studies on characterizing the achievable secrecy capacity of multi-antenna systems performed in [96]–[98], as shown in Fig. 8, have inspired the design and development of many spatial domain-based security techniques.

Antennas: In [103], authors proposed ZF based precoding. The basic idea is to transmit the signal in the null space of the eavesdropper channel. The secure precoding based on ZF beamforming requires both 1) the number of Bobs antennas is larger than that of Eve, and 2) full channel knowledge of Bob and Eves links to the transmitter. In [99], Alice used GSVD

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2018.2878035, IEEE Communications Surveys & Tutorials

TABLE VI
CHANNEL-BASED ADAPTATION TRANSMISSION (SPACE DOMAIN (MULTI-ANTENNA))

Authors	Year	Contributions and Concepts
A. Khisti *et al.* [99]	2007	General SVD of the Bob and Eve channel matrices is used to provide secure communication. There is a trade-off between complexity and performance.
Z. Li. *et al.* [100]	2007	The Bob and Eve's channels are divided into various sub-parallel channels by using some mathematical algorithms such as Gram-Schmidt process.
S. Shafiee *et al.* [101]	2007	The direction of beamforming is tuned and made orthogonal to the direction of Eve's channel as much as possible and tuned towards the direction of the channel of Bob as close as possible.
M. P. Daly *et al.* [102]	2009	DM based security technique is proposed in which the constellation points maintain their positions relative to each other in the desired direction, while they become scrambled in the amplitude and phase at the undesired directions.
A. Khisti *et al.* [97]	2010	Sub-channels of a MIMO system are separated into two different subspace groups. Most of the transmission power is allocated to the subspace intended for legitimate receivers.
Z. Rezki *et al.* [103]	2011	The signal is transmitted in the null space of the Eve. ZF based technique is simple but it has poor secrecy performance.
A.Mukherjee *et al.* [104]	2011	The optimal beamforming design is obtained without depending on the idealized assumption of acquiring Eve's CSI.
H. Reboredo *et al.* [27]	2013	A precoding matrix is designed to minimize the mean square error at Bob only. There is a balance between complexity and performance.
N. Valliappan *et al.* [105]	2013	ASM based security scheme is proposed in which the effective channel appears to be deterministic with respect to Bob, but completely fast fading with respect to the eavesdropper.

TABLE VII
CHANNEL-BASED ADAPTATION TRANSMISSION (SPACE DOMAIN (RELAYS))

Authors	Year	Contributions and Concepts
J. Zhang *et al.* [106]	2010	The employment of cooperative relays (decode and forward) to form a beamforming system to enhance secrecy capacity is introduced.
H. M. Wang *et al.* [107]	2013	A beamforming system based on collaborative use of relays (amplify and forward) is designed to maximize the secrecy capacity.
K. H. Park *et al.* [108]	2013	Three methods for power allocation schemes are proposed based on the available channel state information in order to minimize the outage probability of secrecy rate.
Y. Liu *et al.* [109]	2015	Four relay selection methods are proposed and compared for secrecy enhancement, namely best relay and no jammer, random jammer and best relay, best relay and best jammer, and random relay and random jammer.
H. Hui *et al.* [110]	2015	Two jammers and relay selection schemes are proposed to be used jointly for minimizing the secrecy outage probability.

based beamforming technique in order to decompose both the legitimate channel and illegitimate channel into parallel independent subchannels. The parallel sub-channels can be selected freely and can be encoded separately. In [97], Khisti *et al.* proposed a secure design that uses generalized singular value decomposition (GSVD)-based precoding to establish a transmit matrix to separate the sub-channels of a MIMO system into two different subspace groups. The first one is only for intended receivers, and the second one is for both intended receivers and eavesdroppers. Most of the transmission power was allocated to the first subspace, and only a small portion of the power is allocated to the second subspace. With this power allocation scheme, secrecy message is transmitted through the channel when its gain is higher than that of Eve, while the quality of the Eve's received signals is significantly reduced. In this way, the secrecy capacity of the MIMO system is improved. In [104], Mukherjee *et al.* utilized multiple antennas for beamforming in order to enhance the achievable secrecy capacity of wireless transmission from a source node to a trusted destination node in the presence of Eve as presented in Fig. 9. In [104], authors obtained the optimal beamforming design without depending on the idealized assumption of acquiring Eve's CSI. In [27], Reboredo *et al.* designed a precoding (beamforming) matrix to minimize the mean square error (MSE) between Alice and the Bob, while assuring that the MSE of Eve stays above a given threshold to achieve a certain targeted secrecy capacity.

The work in [111] provided an alternative precoding design based on the quality of service (QoS) metric along with SINR. The scheme includes an optimal regularization parameter and power allocation scheme, both of which also achieve a tradeoff between maximizing signal to interference and noise ratio at Bob (SINRb) and minimizing signal to interference and noise ratio at Eve (SINRe).

As known in the literature, MISO is a special case of MIMO; and due to the reduction in the number of receive antennas to only one single antenna, MISO systems are relatively much simpler than MIMO systems. Orthogonalization-based beamforming is an important type of security techniques for MISO systems. In this technique, the legitimate channel and

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2018.2878035, IEEE Communications Surveys & Tutorials

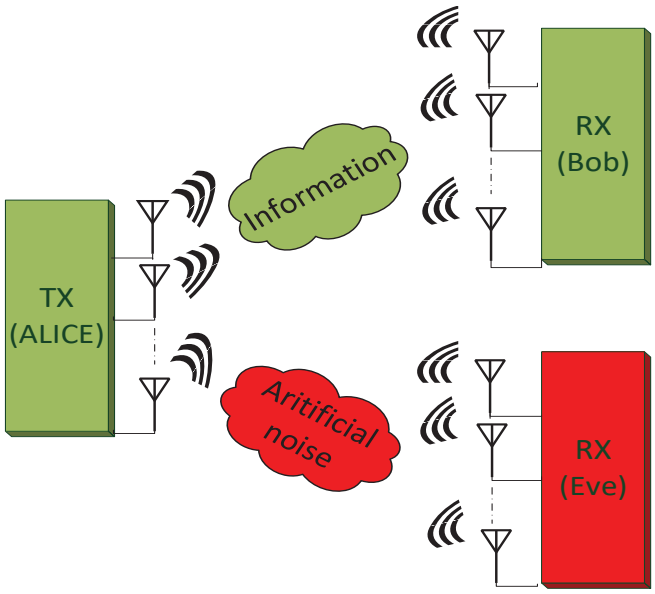

Fig. 8. A MIMO wireless system with Alice, Bob and Eve, each having multiple antenna, $N_{tx} > N_{rx}$.

Eve's channel are divided into various sub-parallel channels by using some mathematical algorithms such as Gram-Schmidt process [100]. The beamforming obtained by this technique is optimal for any value of SNR. At high SNR values, the optimal direction approaches to zero forcing, where the beamforming is tuned towards the direction of Bob, but orthogonal to Eve. In a low SNR region, it means that the average total power is constrained. In [101], the authors presented a sub-optimal solution for beamforming. In this technique, the direction of beamforming is adjusted in such a way that it can be tuned and made orthogonal to the direction of Eve's channel as much as possible and tuned towards the direction of the channel of legitimate receiver as close as possible.

The authors in [102] proposed a directional modulation (DM) technique using a phase array for physical-layer secure communication, which synthesizes the digital modulation symbol in the radio frequency (RF) portion (by using phase shifters) of the transmitter. The basic concept of directional modulation for PLS is presented in Fig. 10. In this scheme, the constellation points maintain their positions relative to each other as traditional digital modulation symbol in the desired direction, while they become scrambled in the amplitude and phase at the undesired directions. Therefore, Eve's performance experiences degradation due to the directional information of the desired receiver even if Eve receives similar signal power. In [112], researchers designed a similar DM signal using an array with pattern-reconfigurable elements.

The authors in [113] and [114] introduced a near-field direct antenna modulation (NFDAM) technique, which forms a DM signal by both a transmit beam and a reflected beam. The reflected beam has an appropriate phase and amplitude by designing the reflector's effective length and scattering properties, which are suitable for synthesizing a DM signal at the desired direction. It should be clear that the DM techniques proposed in the literature have the characteristic of low probability of interception (LPI), which means that eavesdroppers cannot extract any useful information data from the received signal.

Another way for realizing DM transmission is the antenna subset modulation (ASM) introduced in [105]. In this technique, for each transmitted symbol, only a few antenna elements out of the total available number of antennas are selected to beam-form the transmitted symbols toward the direction of the legitimate receiver. The antennas utilized in transmission are randomly chosen for each transmitted symbol to deliver a randomized constellation diagram in the undesired directions (i.e., the antenna switching rate is equal to the symbol transmission rate). In other words, the effective channel will appear to be deterministic with respect to the legitimate receiver, but completely fast fading with respect to the eavesdropper. The resulting artificial fast fading (AFF) behavior will prevent Eve not only from decoding the data symbols received from the antenna side lobes (when Eve is near the transmitter), but also from even estimating his channel.

In [115], authors developed an array processing based directional modulation technique that not only enhances the physical layer security but also enables the receiver to harvest the energy by using co-channel interference. In this work, the authors optimized the array steering vectors to enable direction-dependent modulation with respect to legitimate receiver and showed that the proposed technique can help separate the interference from the desired signal in a spectrally efficient way, and also assist in diverting the energy of interference for harvesting.

Moving away from DM to distributed antenna systems (DAS), which provide wireless transmission and reception system within a geographical location. Authors of [116] proposed a transmit antenna selection scheme for the distributed MIMO

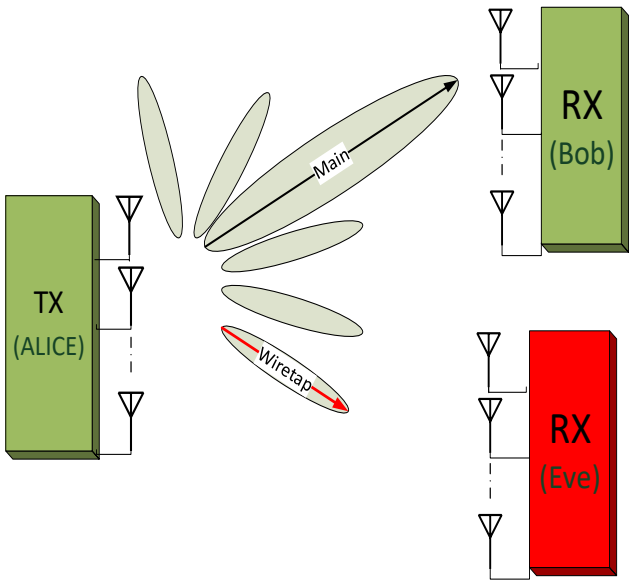

Fig. 9. Secure Beamforming with nulls directed towards Eve.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2018.2878035, IEEE Communications Surveys & Tutorials

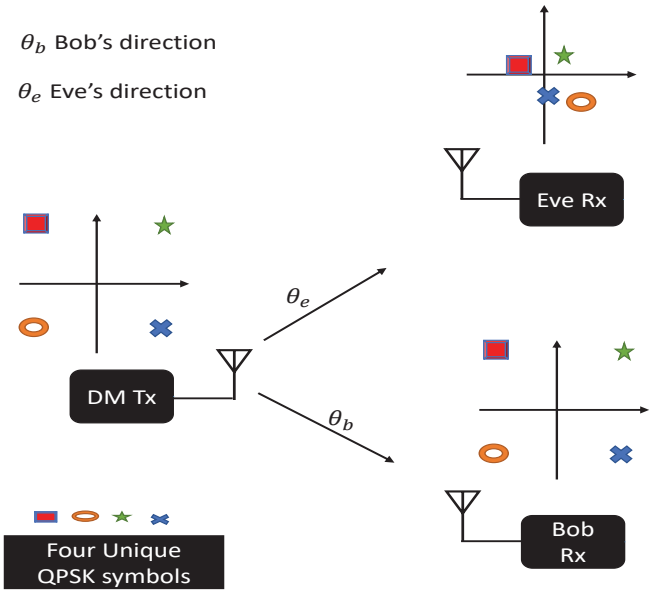

Fig. 10. Physical layer security using directional modulation.

systems. In [117], two combined antenna selection and beamforming schemes: eavesdropper channel nulling (ECN) and distributed phase alignment (DPA), were presented for PLS in distributed antenna systems. In this scheme, two antennas among the available pool are used for the distributed antennas for secure transmission. This is the minimum requirement for the beamforming. In practice, the distributed antennas might have specific power constraints that can affect the scheme. The work also offered DPA which is used to streamline the beams over the conflicted phases in the presence of the eavesdropper at the receiver end. For ECN with an average total power constraint, the authors proposed an analysis model to track the achievable secrecy rate. Numerical results show that ECN exhibits a closed performance as the optimal beamforming with all distributed antennas.

In [118], we investigated the security performance that can be obtained by employing a practical precoded orthogonal space time block coding method (POSTBC) in MISO setup which minimizes the error rate at the legitimate receiver only. The results of POSTBC based precoding show a tangible security gap in the resulting BER performance between Bob and Eve. Moreover, the authors further improved the security of the system by proposing a new precoder design that is composed of both the original precoder and a newly designed unitary matrix that maps Bob's channel amplitudes or phases estimated over the transmitting antennas into 2D orthonormal matrix and called this new technique as precoding along with partial pre-equalizing (PCPPE). The comparative simulation results demonstrate that the PCPPE method provides a better security than using only PMI. Last but not least, many of the interference alignment techniques [119], [120], [121] can be utilized to enhance the security as they inherently have some level of secrecy due to exploiting the knowledge of the channel at the transmitter to reduce interference at only the legitimate receiver.

A brief summary of some of the key contributions related to adaptation in space (antenna) domain is provided in Table VI.

Relays: In the following, we discuss some channel adaptation based PLS techniques for cooperative communication. Generally, cooperative communication is defined as a type of communication system that allows the source to route its data to the destination through a relay placed between the two. The relay creates an additional path for the signal to be transmitted from source to the destination.

In [106], authors proposed the employment of cooperative relays to form a beamforming system depending on the idealized simplifying assumption of having the perfect CSI knowledge of both Bob and Eve's channels and conceived a decode-and-forward relay based beamforming design for maximizing the secrecy rate under a fixed total transmit power constraint. In this scheme, the formulated problem is solved by using the classic semi-definite programming and second-order cone programming techniques. It is shown that the proposed beamforming approach is capable of significantly increasing the secrecy capacity of wireless transmissions. In [122], the authors considered amplify and forward based cooperative communication system to study the advantages of transmit beamforming. It is noticed that the relay improves the performance of source to destination link but it may be untrusted in some cases. To tackle the security problem in untrusted relay, authors presented two secure beamforming schemes, namely a cooperative beamforming and non-cooperative beamforming, where it is demonstrated that beamforming-based techniques outperform the conventional scheme in terms of secrecy capacity.

In [107] paper, a beamforming system based on collaborative use of relays is designed to maximize the secrecy capacity. Perfect channel state information is assumed and amplify and forward relaying protocol is considered. The system is analyzed for both total and individual power constraints by solving the proposed problems using second-order cone programming and classic semi-definite programming techniques. It is shown that the proposed technique can significantly increase the secrecy capacity of the system. In [108], the authors proposed three methods for power allocation schemes based on the available channel state information in order to minimize the outage probability of secrecy rate. In [109], authors proposed and compared four relay selection methods, namely best relay and no jammer, random jammer and best relay, best relay and best jammer, and random relay and random jammer. They derived a new exact closed-form expression for the secrecy outage probability in order to show the joint impact of the proposed relay selection methods and the interference power constraint on the secrecy performance. It is shown that the jammer's absence gives rise to the outage saturation phenomenon. In [110], two jammers and relay selection schemes are proposed for minimizing the secrecy outage probability. In these methods, each node knows its purpose while the purpose of each node is kept secret from Eve. It is shown that maintaining the privacy of jammer's selection and relay node improves the secrecy outage probability performance.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2018.2878035, IEEE Communications Surveys & Tutorials

A brief summary of some of the key contributions related to adaptation in space (relay) domain is provided in Table VII.

Lesson 2: Most of the aforementioned studies related to adaptation-based security whether in time, frequency, or space domain, focus on the optimization of the physical layer transmission parameters according to the channel characteristics without considering the adjustment of the upper layer parameters based on the secrecy requirements. More precisely, the concept of cross-layer security design including the interaction between different layers is not yet well studied in the literature from physical layer perspective. This motives dedicating some of our research efforts as researchers on the following new security concepts. 1) Cross MAC-PHY layer security: In this concept, the MAC functionalities including HARQ, multi-user multiplexing, scheduling, channel accessing, resource allocation control, and prioritization along with the physical parameters can be jointly optimized to maximize secrecy while meeting the basic QoS requirements of the legitimate users. Example on a study related to this new topic can be found in [123], in which ARQ functionality and artificial noise are jointly designed to defend against eavesdropping. 2) Cross NET-PHY layer security: In this concept, the network layer functionalities including routing path determination, amplification with forwarding (relaying), and switching from port (or node) to another along with the physical parameters can be collectively designed to optimize secrecy in the network. Example on a study related to this new topic can be found in [124], in which secure and power-efficient routing protocol is designed to provide confidentiality against multiple eavesdroppers. 3) Cross APP-PHY layer security. In this concept, the transmission parameters of the physical layer are adjusted not only based on the channel but also based on the running applications at the user side and their sensitivity to error and data rates in such a way that improves the overall secrecy. An example on APP-PHY security is application based adaptive modulation along with ARQ [32]. In this scheme, the application can be voice, video, etc. whereas the physical layer parameter is the modulation order along with the number of allowed retransmissions that can be adaptively changed based on the packet error rate value required for a legitimate user to just be able to use the application reliably, while Eve's packet error rate is made not sufficient for reliable decoding of the application.

C. Addition of Artificially Interfering (Noise/Jamming) Signals along with the Transmitted Signals [III]

Concept: The starting point of this direction was sparked and established by Goel and Nagi in [125]–[127], where Eve's channel is made artificially degraded by injecting artificial noise (AN). This approach takes its effect when a trusted node (like Alice, Bob, or third part) adds an intentionally interfering signal (called artificial noise or jamming) that affects Eve's channel severely. This is usually performed by exploiting the null space of the legitimate user's channel that must have some degree of freedom. When there are no nulls in the channel, the transceiver structure including combiners, equalizers, filters, precoders, full-duplex, etc. can be exploited along with the help of diversity for adding well-designed artificially interfering signals that can only harm the eavesdropper [128]. Since in the later case the artificial noise is added without relying on having null space in the channel, the added noise can be named as *null-space independent artificial noise*, whereas the added noise in case of having channel nulls can be named as *null-space dependent artificial noise* as can be found in our work presented in [123].

Merits: The good news about this approach is that, the stringent *perfect secrecy* notion based on Shannon's definition and without using shared secret keys can be achieved in a fading or non-fading environment at any distance Eve may be located at. Thus, it is practically possible and feasible by using a proper, judicious, and intelligent design to make the secrecy capacity exactly equal to the main channel capacity (zero information leakage to Eve). Also, similar to the adaptation-based security approach, this one too does not usually require any extra processing at the receiver side, resulting in reducing complexity and assuring compatibility with the current available handset devices. Additionally, the approach can be applicable to both FDD and TDD systems. Besides, the added interfering signals can be exploited and redesigned to provide additional benefits alongside secrecy such as reducing the peak to average power ratio (PAPR) and mitigating adjacent channel interference and out-off-band emission (OOBE) as can be seen in our work discussed in [123].

Demerits: On the other hand, injecting interfering signals along with or on top of the data signal requires in most cases CSI knowledge at the transmitter. Also, it sacrifices some power resources, and it might degrade the main channel capacity and consequently throughput since some of the degree of freedom is usually scarified for the sake of providing security. Moreover, it might deteriorate the legitimate receiver's performance since it is sensitive to channel estimation errors, and it may also cause PAPR increase if the artificial noise signal is not properly designed. Most importantly, the security level of this method is strongly conditioned upon the assumption that the degree of freedom at the transmitter (Alice) is higher than that at the receiving parties (Bob and Eve) for the null space-dependent approach.

In the following, we review some of the main works, techniques, and studies related to this subject according to the specific type of signal domain (i.e., time, frequency, or space) that the method is exploiting.

1) Time Domain Security: In this domain, the designed interfering signal is added on top of the information signal in time domain such that it gets canceled at only the intended receiver, while causing severe degradation to the eavesdroppers. The added signal can be removed when it passes through the channel itself, or the combiner/equalizer at the legitimate receiver side. However, if the interfering signal remains after passing through the channel and equalizers (filters), then extra processing and/or pre-knowledge of what was transmitted is needed at the receiver side to cancel the added interfering signals. In general, extra processing and pre-knowledge at the receiver side cause signaling overhead and complexity, and also result in changing the receiver structure.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2018.2878035, IEEE Communications Surveys & Tutorials

TABLE VIII
ADDITION OF ARTIFICIALLY INTERFERING SIGNALS ALONG WITH THE TRANSMITTED SIGNALS (TIME DOMAIN)

Authors	Year	Contributions and Concepts
Qin *et al.* [129]	2013	AN is properly designed and added on top of the OFDM signal in the time domain in such a way that when it passes through channel, it gets accumulated over the CP at Bob only.
Y. Yang *et al.* [130]	2015	Multi-path propagation and MRC process with rake receiver are jointly exploited to add AN signals on top of the symbols of each data frame in the time domain.
W. Liu *et al.* [131]	2016	AN approach proposed in [129] is used along with the optimization of a transmit filter that is added just before CP in OFDM system to maximize secrecy.
M. Hussain *et al.* [132]	2016	AN-aided scheme that exploits the null space created by the up-sampling and down-sampling processes is proposed.
J. M. Hamamreh *et al.* [123]	2018	The retransmission process in ARQ protocol is exploited along with MRC at the receiver to provide security even when the channel has only one tap.

Thus, from practical perspective, performing extra processing at the receiver to cancel the noise is not recommended.

Here, we list some of the works performed in this domain. In [129], Qin *et al.* proposed a new AN generation technique, which is performed in time domain instead of space domain (MIMO systems). In this technique, which assumes OFDM as a transmission scheme, the AN is properly designed and added on top of the OFDM signal in the time domain in such a way that when the AN passes through the frequency selective channel, it gets accumulated (collected) over the cyclic prefix (CP) part of the OFDM signal at only the legitimate receiver as presented in Fig. 11. Thus, Bob can automatically (without any extra processing) get rid of this artificial noise signal during the process of removing (discarding) the CP part of the OFDM signal.

On the other hand, Eve, whose channel response is different from that of Bob, will experience interference and thus performance degradation since the artificial noise is designed to be function of the Bob's channel by exploiting the redundancy and degree of freedom derived from cyclic prefix (CP). Since this technique uses the temporal degrees of freedom, the number of transmit antennas does not need to be larger than that of the receive antennas. Later, this method was extended by the same authors to the case of multiple user scenario [133]. It should be mentioned that similar designs are also used to reduce PAPR and OOBE in OFDM systems as can be seen in [134] and [135].

In [131], the authors utilized the temporal AN approach proposed in [129] along with the optimization of a transmit filter added in the time domain just before CP addition process in OFDM system, in order to maximize secrecy while maintaining certain QoS performance level at the legitimate receiver.

In [130], Yang *et al.* introduced a new AN-based secure transmission scheme for single-antenna systems where the multi-path propagation and MRC process with rake receiver are jointly exploited to add AN signals on top of the symbols of each data frame in the time domain. Particularly, the added AN, which is function of the channel of the legitimate receiver, is properly designed to totally remove the inter-symbol-interference (ISI) between data symbols while ensuring full multi-path diversity.

In [132], the authors presented an AN-aided scheme that exploits the null space created by the up-sampling and down-sampling processes. Specifically, the AN is produced and added at the transmitter side after pulse shaping process (after up-sampling) in such a way that it becomes zero at the decision making instances (i.e., sampling times) at the output of matched filter (after down-sampling) of only the legitimate receiver while degrading Eve's performance.

It should be mentioned that the aforementioned time domain AN-based schemes for SISO systems are applicable only when the channel is dispersive due to multi-path. Besides, their secrecy performance highly depends on the number of multiple taps in the channel. In other words, when the channel has a single tap, non of the above schemes can provide secrecy. To overcome this problem, in [123], we proposed a new AN-based scheme that exploits the retransmission process in ARQ protocol along with MRC at the receiver to provide security even when the channel has only one tap. Particularly, a specially designed AN is added on top of each transmitted data packet. If the same packet is requested by Bob, an AN canceling signal is designed and added to the next retransmission round. Then, an AN-free packet is obtained at the legitimate receiver by using MRC process, whereas the AN significantly deteriorates the performance of Eve. The design structure of this ARQ with AN scheme is briefly visualized in Fig. 12. In [137], the

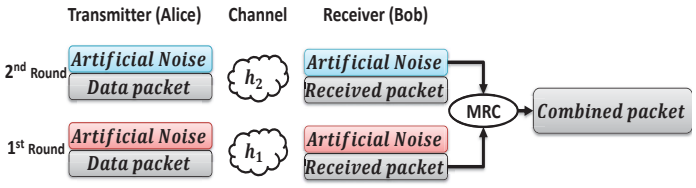

Fig. 12. Design structure of ARQ with AN scheme proposed in [123].

authors introduced a new AN injection method for securing wireless transmission against eavesdropping in quasi-static fading channels. In this method, Bob first broadcasts pseudo random AN towards Alice, who then forwards the received pseudo random AN signal along with the information-bearing signal to Bob. Since Bob knows the generated AN, he can just discard it and then decode the data, whereas Eve, who is assumed to be unable to know the AN signal, cannot decode

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2018.2878035, IEEE Communications Surveys & Tutorials

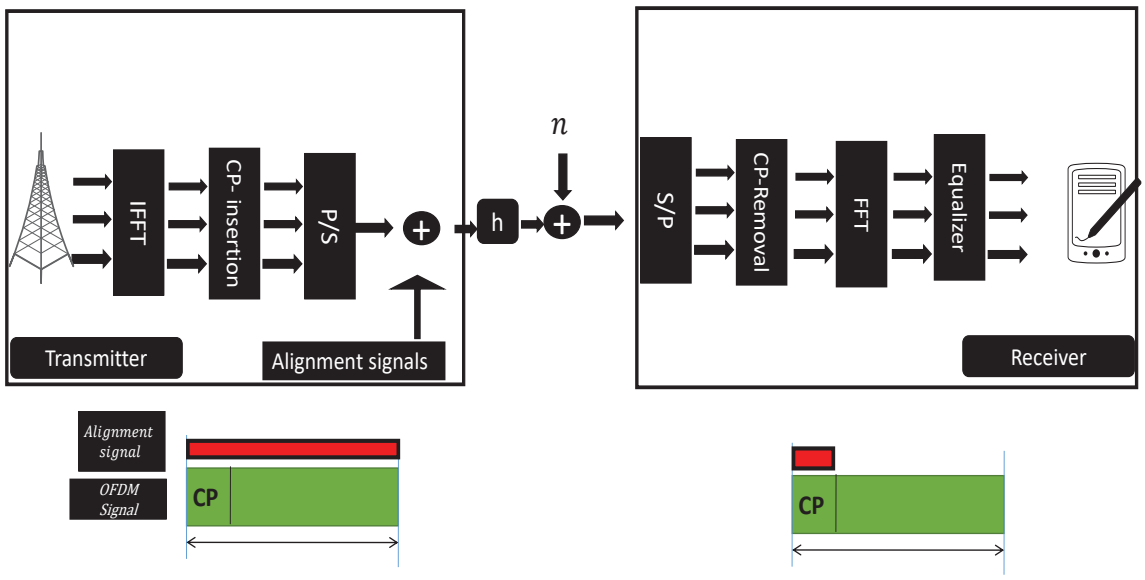

Fig. 11. System model of an OFDM transceiver structure with artificial noise (AN) addition (superposition) in the time domain (after IFFT) of the signal in such a way that the AN aligns after passing through the channel over the CP part that gets discarded with the AN before FFT process at Bob only.

TABLE IX
ADDITION OF ARTIFICIALLY INTERFERING SIGNALS ALONG WITH THE TRANSMITTED SIGNALS (FREQUENCY DOMAIN)

Authors	Year	Contributions and Concepts
E. Guvenkaya *et al.* [79]	2014	The deep-faded frequency sub-channels of the legitimate receiver are filled with artificial noise signals instead of data to confuse the eavesdropper.
T. Akitaya *et al.* [136]	2014	AN generation technique is proposed that is independent of the number of antennas at the transmitter and the length of CP .

the data due to the interference caused by the AN.

A new time domain effective security technique termed as iJam was proposed in [138]. The main idea behind this concept is as follows: At time $t = t_0$, the transmitter sends an OFDM time domain signal (which is composed of N time domain samples, where each sample is generated by a linear combination of N BPSK modulated symbols), while the receiver simultaneously at the same time sends a signal composed of random $Q < N$ jamming samples[6]. In the next time at $t = t_1$, the transmitter repeats transmitting the same OFDM signal that was already transmitted at $t = t_0$, whereas the receiver simultaneously sends a complementary signal composed of $(N - Q) < N$ jamming samples in order to interfere with the samples that were intact at time $t = t_0$. In this technique, the jamming signal is designed in such a way that it does not change the structure of transmitted signal and thus making Eve unaware of which signal samples are jammed and which ones are not. Therefore, Eve cannot correctly decode the received data. On the other hand, since Bob knows ahead of the time positions of the samples he jammed, he can select the correct samples from the signal sent in the first and second time and reorder them to have an intact decodable signal. The good thing about this technique is that it does not rely on the variations of the channel (i.e., channel independent) and can be used to generate and share secret key with high rates. However, the technique suffers from being limited to OFDM with BPSK signaling and also causes throughput degradation and delay.

A brief summary of some of the key contributions related to the addition of interfering signals alongside the data in time domain is provided in Table VIII.

2) Frequency Domain Security: In this domain, the designed interfering signal is added on top of the information signal in frequency domain in such a way that it gets canceled at only the intended receiver, while causing degradation to the eavesdroppers. In [79], the authors proposed a secure communication scheme for OFDM systems operating over multipath channels. In this method, the deep-faded frequency sub-channels of the legitimate receiver are not used for conveying information, but instead filled with artificial noise signals to confuse the eavesdropper. Since Eve has a different channel than that of the legitimate receiver, her deep-fades sub-channels are different from that of the legitimate receiver and thus she cannot distinguish the subcarriers filled with artificial noise from those used to carry data symbols. Therefore, a severe reduction in the eavesdropper channel capacity and performance, which is proportional to the sub-channels filled

[6]Note that the receiver in iJam technique does not use in-band full-duplex structure, but rather a normal half duplex receiver structure as it is synchronized to receive samples from the transmitter at certain samples' indices or positions of the time domain signal, while transmitting time domain jamming samples at the complementary of the positions of the received samples.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2018.2878035, IEEE Communications Surveys & Tutorials

with artificial noise, is achieved.

In [136], authors proposed an artificial noise (AN) generation technique for secure communication in MIMO-OFDM systems. This technique can generate AN at the transmitter side and then removed in the frequency domain at the legitimate receiver side. This is different from the conventional time-domain AN [129] that is canceled out in the time domain at the receiver. The interesting thing about this proposed technique [136] is that it can generate AN irrespective of the number of transmit antennas and the length of cyclic prefix, while the conventional AN generation techniques are constrained on these parameters, which provide the needed degree of freedom. Thus, we notice that this area of research is still very fresh and there are great opportunities for physical layer security researcher and designers to bring the artificial noise-based security concept to frequency domain.

As noticed from the literature, there are very little works done in this domain and somehow in an indirect way. This motives developing more effective techniques tailored to frequency domain to defend against eavesdropping.

A brief summary of some of the key contributions related to the addition of interfering signals alongside the data in frequency domain is provided in Table IX.

3) Space Domain Security: There is a large amount of works done in this domain based on the concept of artificial noise and interfering signal injection concept proposed by Goel and Negi in [125]–[127]. The developed security techniques span most of the space domain scenarios such as MIMO, MISO, SIMO, relays, CoMP, DAS systems. etc.

Antennas: In this subsection, we discuss the main multi-antenna based noise/interference assisted physical layer security techniques. In [127], Goel and Negi introduced artificial noise concept using multiple antennas for generating synthetic noise for enhancing secrecy, especially when Eve's channel is not known at the transmitter and Eve is aware of the legitimate channel link, which is the case in FDD systems that use explicit channel feedback. For this technique to work, there are two conditions that must be satisfied: 1) the number of transmit antennas at source node has to be greater in number than that of the legitimate receiver to ensure having null space in the channel and that the synthetic noise would not degrade the desired channel; 2) the number of antennas at Eve must be less than that at the transmitter to make sure that Eve cannot align the added noise, where a detailed analysis of the effect of Eve's antennas number on the secrecy performance was given in [139]. Interestingly, the authors of [140] conceived the injected AN as a one-time pad unshared secret key that can achieve perfect secrecy at the physical layer, while aligning the AN in the null space of the legitimate channel.

The full MIMO with the injection of artificial noise by using a single multi-antenna helper was investigated in [141]. The strategy of jamming with a multi-antenna helper alongside energy harvesting from the transmitted jamming signal was optimized in [142]. In [143] and [158], orthogonal blinding, another AN pre-coding technique was introduced to achieve positive secrecy in MIMO communication systems, where a transmitter requires at least two antennas to send noise into an orthogonal channel of the main channel by precoding. At the first phase of this technique, Alice computes the channel matrix of Bob's channel using the Gram Schmidt procedure, making each row orthogonal to its counterpart. Then, Alice combines them into a single channel matrix. Due to the available power constraint, a zero forcing filter is used to reduce the channel interference at the output, while ensuring that the intended signal is delivered successfully to only its desired receiver.

MISO scenarios are relatively simpler compared to the aforementioned MIMO scenarios. The channel conditions are easier to determine because transmitters usually have more antennas and more degrees of freedom and higher diversity gains. In [144], authors studied the joint use of artificial noise generation and spatial beamforming for enhancing security of MISO channel in the presence of multiple eavesdroppers given that no CSI of wiretap channel is available. The optimal power allocation, under a specific value of secrecy probability requirement, between the information signal and noise was also examined. The conclusion of this work is that by using both artificial noise and beamforming techniques, both the reliability and security of transmission can be enhanced substantially. The previous work is based on the assumption that CSI is available at the transmitter but in many cases it is difficult to get the CSI of eavesdropper.

In [96], authors proposed a scheme that only require the CSI of Bob's channel. In this scheme, secrecy messages are encoded by using wiretap codes and transmitted in the direction of legitimate receiver channel, while it simultaneously transmits artificial noise in all orthogonal subspace of intended direction. The messages are in the dimension visible to intended receiver, while potential eavesdroppers always receive the mixture of noises and signals. Even if the eavesdroppers have multiple antennas they are still not able to improve their performance. In the literature, there are hybrid techniques that utilize more than one dimension (domain) to further enhance secrecy. For instance, in [147], both the spatial and temporal dimensions are exploited to inject AN in MISOSE-OFDM systems. In this work, AN-based on conventional spatial null-space of the legitimate channel [127] is added to the pre-coded data in frequency domain to confuse Eve. Moreover, before transmission of each OFDM-block, pre-coded temporal AN signals [129] are also added to the signal containing both spatial AN and data. Thus, this technique provide security by using both temporal and spatial null spaces. Furthermore, the authors also investigate the power allocation between the temporal and the spatial AN and the power allocation between the data and the AN. The author extended the MISOSE-OFDM work introduced in [147] to MIMOME-OFDM in [148].

It should be mentioned that there are many works in the literature on this domain, most of these works essentially utilize the original scheme proposed by Goel and Nagi [127], but in different scenarios and channel conditions, and with modified goal functions and metrics to meet different requirements.

In [159] and [146], a new secure transmission scheme called *randomized beamforming* that produces a time varying multiplicative noise to prevent eavesdropping was proposed. In this scheme, random variable coefficients (i.e., noise samples) drawn from complex Gaussian distribution are assigned to the

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2018.2878035, IEEE Communications Surveys & Tutorials

TABLE X
ADDITION OF ARTIFICIALLY INTERFERING SIGNALS ALONG WITH THE TRANSMITTED SIGNALS (SPACE DOMAIN (MULTI-ANTENNA))

Authors	Year	Contributions and Concepts
S. Goel *et al.* [127]	2008	AN concept using multiple antennas for enhancing secrecy is proposed.
A. Khisti *et al.* [96]	2010	Messages are encoded using wiretap codes and transmitted in the direction of legitimate receiver channel, while simultaneously transmitting AN in the orthogonal subspaces of intended direction.
S. A. A. Fakoorian *et al.* [141]	2011	MIMO system with the injection of AN by using a single multi-antenna helper is investigated.
A. Mukherjee *et al.* [142]	2012	The strategy of jamming with a multi-antenna helper alongside energy harvesting from the transmitted jamming signal is investigated.
N. Anand *et al.* [143]	2012	A pre-coding based AN technique is introduced to achieve positive secrecy in MIMO communication systems.
J. Huang *et al.* [144]	2012	The joint use of AN and spatial beamforming for enhancing security of MISO channel in the presence of multiple eavesdroppers is studied.
W. Li *et al.* [145]	2012	The full-duplex receiver is exploited to send jamming signals while receiving its corresponding signal from the transmitter thus providing secure communication.
Q. Li *et al.* [146]	2013	A secure transmission scheme called *randomized beamforming* is proposed that produces a time varying multiplicative noise to prevent eavesdropping.
A. E. Shafie *et al.* [147]	2016	The spatial and temporal dimensions are exploited together to inject AN in both frequency and time domain.
A. E. Shafie *et al.* [148]	2017	The author extended the MISOSE-OFDM work introduced in [147] to MIMOME-OFDM.
M. Soltani *et al.* [149]	2018	The secrecy of randomized beamforming scheme is further enhanced by combining it with the generalized optimal antenna selection schemes.

TABLE XI
ADDITION OF ARTIFICIALLY INTERFERING SIGNALS ALONG WITH THE TRANSMITTED SIGNALS (SPACE DOMAIN (RELAYS))

Authors	Year	Contributions and Concepts
E. Tekin *et al.* [150]	2006	An interesting interference technique in which the transmitted interference signals are independent of the intended message is proposed.
E.Tekin *et al.* [151]	2007	A user (helper), who has a better channel to Eve than that with respect to Bob, ceases sending message carrying signals and instead helps the legitimate receiver by sending i.i.d. Gaussian noise signals to Eve.
L. Lai *et al.* [152]	2008	Noise forwarding technique is proposed that uses cooperative jammer to transmit randomly chosen code-words from a predefined code-book to confuse Eve.
X. He *et al.* [153]	2008	An untrusted relay is jammed with the help of an external node or the intended receiver in such a way that it helps in reliability but cannot extract information from signal.
X. He *et al.* [154]	2009	Well-structured jamming signals are proposed that can degrade Eve's performance without affecting the legitimate receiver's performance.
J. Xie *et al.* [155]	2012	An alignment-based security technique is proposed in which each cooperative jamming signal is aligned with a message signal at the eavesdropper such that it cannot decode it.
Y. Liu *et al.* [156]	2013	A destination assisted jamming technique for AF based cooperative communication system is introduced to provide security.
Q. Xu *et al.* [157]	2017	AN-based waveform design for enhancing PLS of AF relay-assisted CPS system is proposed.

first $N-1$ elements of the beamforming vector (where N is the number of transmit antenna), while the last element of this vector is chosen in such a way that it cancels the added multiplicative noise and makes the channel look deterministic and aligned in the direction of the legitimate receiver only. The scheme is shown to be capable of banning Eve from estimating her channel with respect to the transmitter even if she uses blind channel estimation techniques.

In [160], the authors revisited the randomized beam-forming concept and renamed it as *artificial fast fading (AFF)* because the effective channel with respect to the eavesdropper appears fast fading (equivalent to non-coherent Ricean fading channel). A detailed secrecy performance comparison between the AN and AFF techniques was introduced and it is observed that the secrecy performance of AFF scheme is less than that of the AN scheme when the transmitter has more antennas than that of the eavesdropper; whilst the AFF scheme attains much better secrecy when the eavesdropper has more antennas than that of the transmitter. Specifically, when the number of antennas at Eve is double that of the transmitter, the AFF scheme maintains its applicability unlike the AN scheme that does not function under this situation. Consequently, the AFF scheme is more immune and resilient to eavesdroppers with multi-antenna. Also, the secrecy of randomized beamforming (or AFF) scheme can be enhanced further by combining it with generalized optimal antenna selection schemes [149].

In spite of the effectiveness of the AN and AFF approaches, they have some hurdles, which can be summarized as follows. 1) Spatial degree of freedom (multi-antenna existence) at the transmitter is a must for these techniques to work. 2) the

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2018.2878035, IEEE Communications Surveys & Tutorials

Bob's CSI is required at the transmitter, causing feedback-signaling overhead alongside making the techniques channel-dependent and thus prone to channel estimation and reciprocity mismatch errors. More importantly, for the cases where the transmitter does not have spatial degree of freedom (i.e., a transmitting node with a single antenna due to limitation in size and limited computational capabilities as is the case in IoT applications), neither AN nor AFF can be used to provide guaranteed secrecy. However, security can still be provided by exploiting the transceiver structure of a receiver with *in-band full-duplex* capabilities [145]. Particularly, in this technique, the full-duplex receiver sends jamming signals (that is constantly changing) while receiving its corresponding signal from the transmitter. Since the receiver is the source (originator) of this jamming noise like signal, the receiver Bob can fully cancel this jamming signal as he knows its exact value before transmitting it. On the other hand, any eavesdropper in the region will be severely affected by this generated jamming signal, whose value is not known to Eve, and thus cannot be canceled. The technique can be employed by using a single antenna full-duplex receiver or multiple antenna full-duplex receiver [161], where the jamming signal is generated by utilizing a portion of the available antennas at the receiver while using the remaining portion for receiving data signals simultaneously. The technique is shown to be robust against multiple eavesdropper observations (i.e., colluding/multiantenna eavesdroppers) and capable of achieving perfect secrecy. The fundamental features of providing secure signal transmission using full-duplex transceivers under realistic assumptions has recently been established in [162]. In addition, the real-time practical implementation of a full-duplex-based security scheme with artificial noise has been recently conducted and investigated by using a testbed of software defined radios (USRP devices) in [163].

It should be noted that many works have recently appeared on utilizing full-duplex for PLS, most of the these works are fundamentally similar in the sense that they use the original technique of full-duplex transceiver structure to achieve secrecy but in different scenarios, various channel conditions, and modified goal functions in order to understand, investigate, and evaluate the secrecy performance in a very comprehensive manner.

A brief summary of some of the key contributions related to the addition of interfering signals alongside the data in space (antenna) domain is provided in Table X.

Relays: In this subsection, we discuss the main relay based noise/interference assisted physical layer security techniques. Noise forwarding technique is one of the important PLS techniques that was first described in [152] for the Gaussian relay channel. The technique uses cooperative jammer that transmits randomly chosen (non-information carrying) codewords, which are taken from a predefined code-book instead of transmitting Gaussian noise signal. In this way, the authenticated user can easily decode the confusion signal whereas eavesdropper can not do the same. This is ensured only if the rates are chosen wisely with respect to the legitimate user [152].

In [150] and [164] authors proposed an interesting interference technique in which the transmitted interference signals are independent of the message. However, this technique is limited use cases because the signals become the cause of interference for both the authenticated receiver and the eavesdropper, resulting in a limitation in the decoding capabilities of the authenticated receiver. On the other hand, this technique increases the level of security. According to the method presented in [151], a user (helper), who has a better channel to Eve than that with respect to Bob, ceases sending message carrying signals and helps the legitimate receiver by sending i.i.d. Gaussian noise signals instead.

Another type of techniques is based on adding an independent interference signal into the channel in addition to the message carrying signal. The objective of interference signal is to confuse and disturb Eve's reception by jamming her channel. This signal is designed in such a way that it degrades Eve's performance but have minimum effect on the legitimate receiver [165]. The main difference between cooperative jamming with Gaussian noise and noise forwarding is that in cooperative jamming the most important thing is the appropriate rate that enables the decoding of the confusion signal by the authenticated user who is able to receive a clean signal, whereas Eve is not able to separate information carrying signal from confusion signal. However, in noise forwarding, both the authenticated user and eavesdropper's signals are hurt [151], [165]. One of the techniques based on interference is called cooperative jamming by structured codes. The basic issue with Gaussian noise based cooperative security technique is that it also hurts the legitimate receiver.

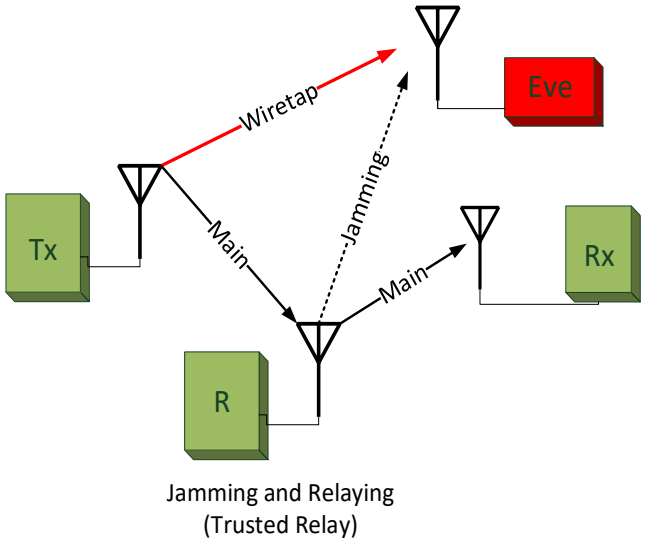

Fig. 13. Cooperative jamming of evesdropper with artificial noise (Trusted relay).

As per [154], the well-structured jamming signals can improve the secrecy level in such a way that it degrades the Eve's performance but it does not degrade the legitimate receiver's performance. Another interesting interference-based security technique is the one based on alignment. In alignment-based technique discussed in [155], each helper node sends

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2018.2878035, IEEE Communications Surveys & Tutorials

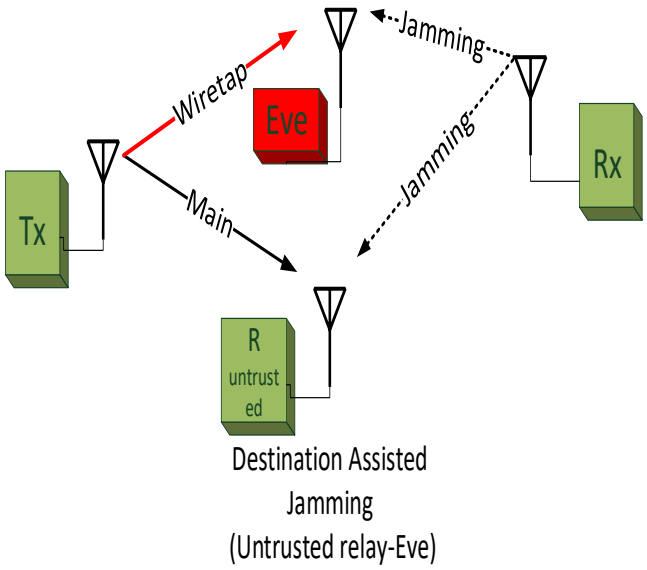

Fig. 14. Cooperative jamming of evesdropper and untrusted relay with artificial noise (untrusted relay).

a cooperative jamming signal based on alignment concept. Particularly, each cooperative jamming signal is aligned with a message signal at the eavesdropper such that it is not separable, hence minimizing the information leakage at the eavesdropper; while cooperative jamming signal are aligned in different separable dimensions at the legitimate receiver.

The basic concept of jamming in cooperative communication in the presence of trusted relay, which is explained in [154], is presented in Fig. 13. In [153], an untrusted relay case is presented in which the relay helps in reliability while being untrusted as shown in Fig. 14. In this case, the relay is jammed with the help of an external node or the intended receiver in such a way that it helps in reliability but cannot extract information from signal. In the method presented in [108], a jamming signal is first transmitted to the eavesdropper by the receiver or the destination and at the same time the source is directed to send information towards the relay. Afterwards, the destination using self-interference cancellation removes the jamming noise. According to [156], a destination aided jamming technique is introduced to provide security by using two phases. In the first phase, the source transmits a signal towards the relay and simultaneously cooperates with the destination for jamming the eavesdropper. In the later phase, the decoded source signal is transmitted by the relay, at the same time; this relay cooperates with the source to jam the eavesdropper without creating interference at the destination.

Cyber-Physical System (CPS) is the integration of networking, computation and physical processes in which the physical processes with feedback loops are controlled and monitored by embedded system. The application of CPS includes smart grid, traffic control and medical monitoring. In [157], the authors proposed PLS techniques for CPS system. In that work, the authors proposed artificial noise based waveform design for enhancing PLS for AF relay-assisted CPS system. In the first step, perfect CSI of Eve was considered and AF coefficient for information signal and AN covariance was optimized for enhancing PLS. Afterwards, authors also considered imperfect CSI case of Eve for more practical scenario.

A brief summary of some of the key contributions related to the addition of interfering signals alongside the data in space (relay) domain is provided in Table XI.

Lesson 3: The aforementioned studies related to artificial noise/interference-based security whether in time, frequency, or space domains, concentrate mainly on maximizing the secrecy capacity without considering or paying much attention to many of the practical constraints that may impede and prevent the practical realization of such approach. Particularity, peak-to-average-power ratio (PAPR) increase caused by the addition of artificial noise (whose distribution is generally assumed to be Gaussian) causes severe problems in terms of operating in the non-linear region of the power amplifiers, resulting in power inefficiency, coverage range reduction, and inter-modulation products generation along with in-band and out-of-band interference. Accordingly, as researchers in this field, we see a necessity to start considering the practical constraints such as PAPR while formulating the secrecy-related optimization problems to make the future proposed schemes more realistic, and thus more likely to be adopted in practice.

D. Extraction of Secret Sequences from Wireless Channels [IV]

Concept: The starting era of this research direction was pioneered and introduced by Bennett *et al.* in their seminal paper titled "privacy amplification by public discussion" [166], where secure key agreement between legitimate nodes is achieved over an insecure channel (Eve has full access to it with non-identical observations to that of Bob). However, the generalization of this concept along with the fundamental theoretical studies of this research direction can be traced back to Maurer in his seminal work described in [167]. Interestingly, Maurer's work happens to be coincidently very similar and close to the work concurrently (but independently) done by Ahlswede and Csiszar in [168] and [169]. The secret key generation analysis made in [167] was extended to account for the presence of an active eavesdropper in [170]–[172]. This security approach takes its effective action when the transmitter and receiver extract random sequences (vectors) or random matrices called secret keys from the channel of the legitimate link, and each side performs some mathematical processing to manipulate (encrypt) the data at Alice and reconstruct (decrypt) the manipulated data at Bob, as briefly presented in Fig. 15[7].

Key generation-driven PLS techniques are based on the following main foundational assumptions. 1) Spatial channel decorrelation, where Bob and Eve, who are located at different positions (at least half-wavelength apart from each

[7]It is worth mentioning that the techniques reviewed in this section are applicable for providing confidentiality as well as authentication.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2018.2878035, IEEE Communications Surveys & Tutorials

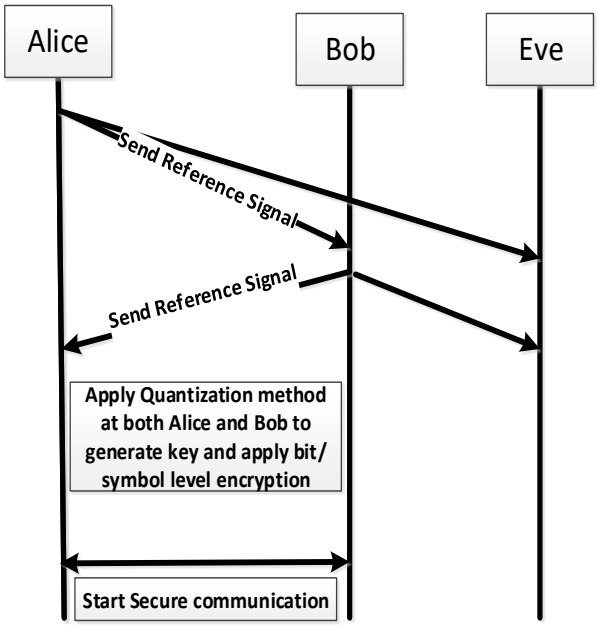

Fig. 15. Generating secret key from the legitimate wireless channel.

other), experience independent channel responses. 2) Channel reciprocity, where similar channels at both ends of the same link are measured so that they can be used to generate similar, common, and shared keys at both ends. 3) Channel randomness (variation) that can exist in the temporal, spectral, and/or spatial domains due to rich scattering environments that cause fading and multi-path reflections.

Temporal channel variation, which is due to the movements of legitimate nodes or other environmental objects, is one of the most common and important source of randomness for increasing the generated key length. Majority of the secret key generation techniques in the literature are based on received signal strength indicator (RSSI), channel state information (CSI) including phase and amplitude, and secrecy wiretap channel codes. The basic steps for key generation include: 1) probing of channel by using sounding techniques to have random correlated measurements at both sides of the communicating parties, 2) extracting channel features to use them as common random variables, 3) performing channel quantization to generate secret random keys, 4) implementing privacy reconciliation to reduce key mismatch, and 5) carrying out privacy amplification to enhance key randomness.

Merits: The research on channel-based key generation and extraction has been established and motivated by two aspects: 1) solving key management problem including distribution, sharing, and storing of keys associated with complexity-based security methods; 2) overcoming the problem resulting from the fact that Eve may have better channel conditions than Bob; 3) reducing complexity compared to public key cryptography.

Demerits: This approach cannot practically achieve perfect secrecy notion defined by Shannon as the number of generated random bits is usually limited by the channel variations, thus it can be broken by Quantum computing[8]. Interested readers are recommended to take a look at the recently published report about this issue by National Institute of Standards and Technology (NIST) [174]. Also, it is mentioned that the channel-based key generation approach is very sensitive to imperfect channel estimation and channel reciprocity mismatch. Thus, it may degrade legitimate receiver performance. To overcome this issue, robust channel calibration techniques are highly needed besides reconciliation approaches that usually require some extra signaling and overhead. Besides, this approach requires extra, add-on processing at both the transmitter and receiver sides, necessitating complex processing that consumes extra power and causes additional delay. Furthermore, this approach is limited to TDD systems where channel reciprocity holds and thus can be exploited to extract random keys. Thus, generating random sequences in FDD systems remains a challenging issue. Finally, when the channel is poor scattering or line of site (LOS), where there is no much randomness and variations in the channel, the secret key rate will be extremely low, making this approach ineffective.

In the following, we review some of the main works, techniques, and studies related to this subject according to the specific type of signal domain (i.e., time, frequency, or space) that the method is exploiting.

1) Time Domain Security: In this domain, the variations of the channel between the legitimate communication parties in time domain due to fading, interference, dispersion and noise are exploited to generate and extract random keys. Thus, keys are extracted via exploiting the common randomness that inherently exists in reciprocal wireless channels, where the channel at the transmitter is the same as the one at the receiver with a possible small mismatch due to the natural imperfect channel reciprocity[9] and estimation errors. In [175], researchers proposed a technique that uses the short term reciprocity of the radio channel to secure information, where the exchange of information does not require the availability of a common secure key between the two users since the phases of the fading coefficients are used as a secret key. The proposed technique can also be used for cryptographic key agreement between two users.

In [176], the authors proposed transmit array optimization to induce more rapid fluctuations in the channel from which keys can be extracted. In [185], a technique, which is directly quantizing the complex channel coefficients, was suggested. In [177], discretizing the extracted coefficients of some practical and standardized multipath components was investigated. Utilizing the crossing rates of the fading channel at the

[8]Many companies (such as Google, IBM, Microsoft and D-Wave) are taking quantum computing and quantum communication very seriously and trying to make it a reality. A recent comprehensive survey on quantum channel communication is available at [173].

[9]Channel reciprocity mismatch problem happens due to the fact that the effective response of the radio frequency (RF) hardware front-end in the downlink is usually different from that of the uplink. Besides, reciprocity mismatch can also occur due to having different interference level in the uplink than that of the downlink.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2018.2878035, IEEE Communications Surveys & Tutorials

TABLE XII
EXTRACTION OF SECRET SEQUENCES FROM WIRELESS CHANNELS (TIME DOMAIN)

Authors	Year	Contributions and Concepts
H. Koorapaty *et al.* [175]	2000	A technique that uses the short term reciprocity of the radio channel to secure information is proposed.
T. Aono *et al.* [176]	2005	Transmit array optimization is proposed to induce more rapid fluctuations in the channel from which keys can be extracted.
C. Ye *et al.* [177]	2007	Discretizing the extracted coefficients of some practical and standardized multipath components is investigated.
Azimi-Sadjadi *et al.* [178]	2007	An interesting key generation that exploits deep fades for quantization of RSSI values is proposed.
T. Kitano *et al.* [179]	2007	BER fluctuations are used for generating channel based secret keys.
S. Mathur *et al.* [180]	2008	Secret bits are extracted from RSSI and CIR measurements using two-level crossing excursion-based quantization.
S. Jana *et al.* [181]	2009	An effective adaptive technique is proposed to extract multiple bits using single measurement of RSSI.
C. Ye *et al.* [182]	2010	Crossing rates of the fading channel are exploited for key generation at the trusted parties.
Y. Abdallah *et al.* [183]	2011	One-bit feedback messages (ACK and NACK) generated by Automatic Repeat Request (ARQ) protocol are explored for key generation.
Shehadeh *et al.* [184]	2011	Key generation scheme is presented in which the phases of channel taps are shifted towards constellation points synchronously.

trusted communicating parties (Alice and Bob) was studied in [182]. Also, the exploitation of the estimated channel as correlated random variables for information reconciliation was investigated in [186]. Exploiting one-bit feedback messages (ACK and NACK) generated by Automatic Repeat Request (ARQ) protocol used in many practical networks such as WiFi was explored for key generation in [183].

In [180], authors extracted secret bits from RSSI and CIR measurements by using two-level crossing excursion-based quantization. They analyzed their algorithm numerically, theoretically and experimentally. Azimi-Sadjadi *et al.* proposed an interesting approach for key generation that exploits deep fades for quantization of RSSI values in [178]. The measurement is encoded as 1 if it is greater than a threshold otherwise 0.

In [181] and [187], an effective adaptive technique was proposed to extract multiple bits by using single measurement of RSSI. The authors also included reconciliation and privacy amplification to remove the mismatch between the generated keys and to enhance the key entropy. They also presented the effectiveness of their scheme by performing real world measurements in different settings. Shehadeh *et al.* [184] proposed phase shifting based secret key generation scheme in which the phases of channel taps are shifted towards constellation points synchronously. The method was shown to have higher key generation rate at low disagreement probability.

In [188], Patwari *et al.* proposed an interesting framework for secret key extractions from radio channel measurements series and called it as High-Rate Uncorrelated Bit Extraction (HRUBE) framework. In their work, non-simultaneous measurements that are inherent in TDD due to half-duplex communication and temporal correlation of oversampled channel measurements are addressed. The framework includes interpolation, decorrelation by transformation and adaptive quantization as main steps. In the first step, multiple channel samples are collected at some instants and fractional interpolation is applied, after that Karhunen-LoKeve transform is used for the decorrelation of channel components and finally an adaptive quantization method is employed to get higher efficiency. They also showed experimentally that their technique can generate secret key rate of 10 bits/sec while having bit mismatch rate of 0.54%. In [179], authors investigated BER fluctuations for generating channel based secret keys. The authors considered BER as an appropriate channel characterization indicator.

A brief summary of some of the key contributions related to channel-based key generation in time domain is provided in Table XII.

Remark: The aforementioned research studies mainly focus on extracting secret keys to be used at the upper layers (with the exception that the keys are extracted from the physical channel), making it somehow similar to conventional upper layer encryption techniques that are prone to brute force attacks at the application layer. However, there are other schemes that use the extracted randomness to manipulate certain transmission parameters associated with the data on a symbol level (instead of bit level) basis at the physical layer. This helps to protect the signal from being detected, demodulated, or decoded properly, making Eve unable to even understand the information-carrying signal at the early stages of the physical layer reception. Example on these schemes that utilize the randomness of the channel to manipulate the data on a symbol level basis (instead of bit level) in the time domain is channel phase-based modulation randomization technique proposed in [189]. Particularly, the authors introduced a PLS scheme in which the modulation type is changed based on the phase of the channel. Moreover, in order to further improve immunity against eavesdropping, the phase of transmitted signal is also rotated. The proposed scheme has shown high level of robustness in the presence of estimation errors.

2) Frequency Domain Security: Similar to key extraction based on time domain channel variations, frequency domain too as another degree of freedom can be exploited for secret key generation. Here, we review some of the works done on this domain, which is closely related to OFDM systems. Quantizing the channel phases for a multi-tone communication

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2018.2878035, IEEE Communications Surveys & Tutorials

TABLE XIII
EXTRACTION OF SECRET SEQUENCES FROM WIRELESS CHANNELS (FREQUENCY DOMAIN)

Authors	Year	Contributions and Concepts
S. C. Draper *et al.* [190]	2011	Quantization of the channel phases to generate secret keys for a multi-tone communication is proposed.
Q. Wang *et al.* [191]	2011	Channel phase-based key generation and agreement over time-varying frequency response channel in OFDM wireless systems is proposed.
Wang *et al.* [192]	2012	A key generation scheme using reciprocity of the time delays and angles of multipath channel for FDD based wireless system is proposed.
C. Y. Wu *et al.* [193]	2013	OFDM sub-carriers along with precoding matrix indices are exploited to generate secret keys.
H. Liu *et al.* [194]	2013	Fast and reliable RSS-based key generation technique for OFDM is proposed for both indoor and outdoor environments.
H. Li *et al.* [195]	2015	Dynamic subcarrier allocation and interleaving based on the legitimate CSI are used to provide eavesdropping-resilient OFDM system.
J. Zhang *et al.* [196]	2016	An effective key generation method by utilizing the unique randomness of the channel responses of multiple individual OFDM subcarriers is proposed.
J. Zhang *et al.* [197]	2016	Experimental work on key extraction from the channel of the legitimate user for PLS in wireless systems is conducted.
W. Cheng *et al.* [198]	2017	Practical implementation of key generation from frequency channel response using USRP radio devices is presented.
J. Zhang *et al.* [199]	2017	A PLS scheme for OFDM systems is proposed in which dummy data is transmitted in several randomly selected OFDM subcarriers.

system such that multiple independent phases are used to generate longer keys was conducted in [190], [200], [201]. On the other hand, the authors of [202] and [191] studied channel phase-based key generation and agreement by using time-varying frequency response channel in OFDM wireless systems. In [203], authors proposed robust quantization mechanisms for key generation to achieve higher secret bit rate. Additionally, practical issues such as delay and mobility, which impact the performance of the key generation process, are thoroughly studied.

In [193], a practical physical layer security methods based on exploiting OFDM sub-carriers along with precoding matrix indices (PMI) are exploited to be used as secret keys. In [204] and [195], dynamic subcarrier allocation and interleaving based on the legitimate CSI are used to provide eavesdropping-resilient OFDM system. In [196], the authors presented an effective key generation method by utilizing the unique randomness of the channel responses of multiple individual OFDM subcarriers. In [205], authors proposed RF-front end based key generation and physical layer authentication for mobile nodes with temporal varying carrier frequency offsets. In [197], an experimental work on key extraction from the channel of the legitimate user for PLS in wireless systems is conducted. Another practical implementation of key generation from frequency channel response by using USRP radio devices is reported in [198].

In [194], authors proposed fast and reliable RSS-based key generation technique for OFDM. The authors exploited the channel state information (CSI) from multiple subcarriers of OFDM for generating secret key for both indoor and outdoor environment by using intel 5300 WiFi card and showed the effectiveness and feasibility of using OFDM for key generation. Furthermore, they also proposed a channel gain complement aided key extraction method to reduce channel's non-reciprocity effects. The technique can achieve secret bit generation rate of 60 to 90 bits per packet, and it is resilient to attacks against RSS based technique, such as stalking attack and predictable channel attack.

In [199], authors presented a less computationally complex physical layer encryption scheme for OFDM systems. The basic idea is based on subcarrier obfuscation where dummy data is transmitted in several randomly selected OFDM subcarriers. In order to prevent Eve from channel estimation and synchronization, the training sequence is replaced with a unique secure training sequence. In [192], Wang *et al.* proposed a key generation scheme for non-reciprocal FDD based wireless system. They considered that time delays and angles of multipath are reciprocal and generated key by quantizing these parameters. Moreover, an error correction scheme was also proposed for reconciliation based on Chinese remainder theorem.

A brief summary of some of the key contributions related to channel-based key generation in frequency domain is provided in Table XIII.

Remark: Similar to time domain, in frequency domain, there are studies that use the generated randomness to encrypt data at the physical layer instead of upper layers. An example on schemes that utilize the randomness of the channel to manipulate the transmitted data in the frequency domain (before IFFT process) on a symbol level basis at the physical layer is given in our work introduced in [83] where the randomness of the channel is used to shuffle, randomize and interleave the subcarrier positions adaptively according to the amplitude of the channel frequency response of the legitimate receiver to prevent eavesdropping.

3) Space Domain Security: In this domain, multiple antennas (including localized and distributed ones), and relays (including trusted and non-trusted ones) are exploited for producing secret keys. Key generation techniques from the spatial domain of the channel are particularly useful and

TABLE XIV
EXTRACTION OF SECRET SEQUENCES FROM WIRELESS CHANNELS (SPACE DOMAIN (MULTI-ANTENNA))

Authors	Year	Contributions and Concepts
A. Kitaura *et al.* [206]	2007	Variations produced by antenna switching are used for key generation. Instead of threshold based method, the signal strength comparison at the antenna is used for this purpose.
Chen *et al.* [207]	2009	A technique for generating uncorrelated secret key bits by using multiple antenna is proposed. Also, channel averaging, least square estimation, LDPC code and gray coding are used to reduce mismatch.
Wallace *et al.* [208]	2010	An intelligent key generation algorithm based on using alternating staggered quantization is proposed.
Zeng *et al.* [209]	2010	RSSI based key generation and multi-level quantization at each antenna for multi-antenna based system is proposed. Furthermore, excursion based quantization and guard intervals are used to minimize errors.
Furqan *et al.* [210]	2016	A practical key generation method based on channel quantization with singular value decomposition is proposed.

effective when a single direct link is not good enough to generate high secret key rates.

Antennas: MIMO wireless technology can considerably increase the channel's randomness. This extra dimension (degree of freedom) can be used for efficient secret key generation. The basic foundations for the theoretical limits of secret key generation exploiting MIMO channel are presented in [218] and [219]. In [208], Wallace *et al.* proposed an intelligent key generation algorithm based on using alternating staggered quantization. The results show that the proposed technique outperform the conventional guard band based quantization. Zeng *et al.* investigated multi-antenna based key generation in real wireless systems [209]. They applied RSSI based key generation and multilevel quantization at each antenna. In order to reduce probability of error, excursion based quantization and guard interval are used. Also, the agreement on the guard interval, the quantization level, the excursion size, the antennas to be used and the RSSI measurements is done by public discussion. Moreover, in order to enhance the entropy of the derived key a simple bit-wise XOR function is also applied.

Chen *et al.* proposed an interesting channel based key generation technique by using multiple antennas in [220] and [207]. The proposed algorithm can generate uncorrelated secret key bits although the channel exhibits spatial and temporal correlation. Furthermore, the authors also presented error reduction algorithms such as channel averaging, least square estimation, LDPC code and gray coding. In [206], a novel antenna switching based key generation algorithm for multi-antenna is explained. More specifically, variations produced by antenna switching are used for key generation and instead of threshold based method, the signal strength comparison at the antenna is used for this purpose.

Furthermore, in [187], authors investigated RSS-based key extraction for MIMO case by using MIMO-like sensor testbed. In order to decrease the bit mismatch and for the performance enhancement, an iterative distillation step is used before reconciliation stage. The basic concept of iterative distillation is to eliminate those kind of measurements that may lead to discrepancies in bits between the legitimate parties. In [193], the authors proposed two practical security techniques for the MIMO-OFDM systems: The first one is based on precoding matrix indicator (PMI) for secret key generation with rotation matrix while the second one is based on channel quantization. The first scheme uses PMI and rotated reference signals in such a way that eavesdroppers are not able to learn information about secret key whereas the second technique applies channel quantization in order to obtain longer secret key. One of the important advantages of the second technique is that the key disagreement probability is significantly reduced and the communication overhead of the public discussion is decreased. In [210], we introduced a practical key generation method based on channel quantization with singular value decomposition (CQSVD), which is shown to be capable of significantly increasing the generated secret key in MIMO systems. We used alternative form of SVD for achieving fine quantization of the phases and amplitudes of the estimated MIMO channel coefficients to increase the length of generated secret key.

A brief summary of some of the key contributions related to channel-based key extraction in space (antenna) domain is provided in Table XIV.

Relays: Relays are attractive candidates for key generation based PLS because they can enhance the key rate and randomness by providing alternate path. Interestingly, both trusted and untrusted relays can be used for key generation techniques [221].

In [222], the key generation of three slots for the two single-antenna nodes with the help of relay has been suggested. The presented scheme uses the concept of the mutual information estimation based on k-nearest neighbor-distance for simulation results. However, the authors did not mention how to generate a key based on the received signals. In a study discussed in [214], the secret key rate (SKR) and key generation scheme using two way relaying is introduced. Particularly, the authors studied key generation problem in two-way relay channel in the absence of any direct path between key generating nodes. They proposed an effective high rate key generation scheme in which correlated observations at the generation nodes are not needed. The authors also analyzed the degradation effect on key generation in the presence of active attacks. According to [211], a scheme aiming at improving the generation of the key via multiple untrusted relays is proposed. In this technique, relays broadcast an XORed version of two keys which are based on the two channels. One channel is between the legitimate users and the relay and the other one is between the two legitimate users. Furthermore, the users make a secret key by combining the known keys and the broadcast keys. However, this scheme cannot work with either multiple colluding relays

TABLE XV
EXTRACTION OF SECRET SEQUENCES FROM WIRELESS CHANNELS (SPACE DOMAIN (RELAYS))

Authors	Year	Contributions and Concepts
L. Lai *et al.* [211]	2012	Key generation via multiple untrusted relays is proposed.
Q. Wang *et al.* [212]	2012	Secret key generation based on trusted relays is introduced.
Wilhelm *et al.* [213]	2013	A protocol for key generation based on frequency selectivity of channel is proposed which does not require mobility of nodes.
H. Zhou *et al.* [214]	2014	The key generation problem in two-way relay channel in the absence of any direct path between key generating nodes is investigated.
Liu *et al.* [215]	2014	RSS based collaborative key generation mechanism for securing communication among a group of wireless devices is proposed.
C. D. T. Thai *et al.* [216]	2016	Secret key generation in the presence of several multi-antenna untrusted relays is proposed for fully, partially, and non-colluding modes.
Furqan *et al.* [217]	2017	Channel independent security technique for an untrusted decode-and-forward (DAF) relay using secret keys and destination-assisted jamming is proposed.

or a single relay case. In [212], authors offered secret key generation based on trusted relays. In this scheme, in order to increase the key generation rate, multiple trusted relays are employed. The authors considered the effect of estimation method on the extraction of secret bits and also derived the theoretical upper bound from Cramer-Rao bound (CRB) and from mutual information of correlated random sources on maximum key rate.

In [223], Kan Chen *et al.* proposed two relay based cooperative MIMO architectures with key generation techniques for each of them. They also quantified the effect of the proposed power allocation on the key generation rate by theoretical and numerical analysis. The authors showed that there is an increase of $15\% - 30\%$ in the key rate of cooperative MIMO networks by using the proposed power allocation scheme as compared to equal power allocation. In [213], Wilhelm *et al.* introduced a protocol for key generation based on frequency selectivity of channel which does not require mobility of nodes for key generation. The authors evaluated the robustness and security of the proposed scheme experimentally by implementing it on MICAz mote modules. The proposed algorithm gives a key agreement rate of over 97% by mitigating temporal effect and errors in measurement. In [215], Liu *et al.* presented a framework to enable secure communication among a group of wireless devices using RSS based collaborative key generation mechanism. They proposed two collaborative key generation algorithms through chain and star topology for secure group communication. The algorithms are implemented experimentally on MICAz motes and shown to be feasible for secure group communication in both outdoor and indoor environments at a lower key mismatch rate compared to existing techniques in the literature.

In [217], we suggested a channel independent and power efficient security technique for an untrusted decode-and-forward (DAF) based cooperative communication system. The technique is based on the concept of switchable untrusted DAF (sDAF) relay and destination-assisted jamming that can help in using untrusted DAF relay to enhance the reliability of the system without enabling it to eavesdrop the information. In [216], authors considered the secret key generation in the presence of several multi-antenna untrusted relays. The authors also elaborated about different modes of colluding such as fully, partially, and non-colluding modes.

A brief summary of some of the key contributions related to channel-based key extraction in space (relay) domain is provided in Table XV.

Lesson 4: The aforementioned studies related to channel-based secret key generation, whether in time, frequency, or space domains, mostly concern and care about extracting higher random key rates from the channel with lower key mismatch probability between the transmitter and receiver, without discussing much about how to use the extracted keys and at which layer they should be utilized. On the other hand, there are other techniques that utilize pre-shared keys at the transmitter and receiver to encrypt the data on a symbol level basis at the physical layer, resulting in what is called physical layer encryption (PLE) [199]. The pre-shared keys can also be used to create: 1) artificial inter-symbol-interference as shown in [224], 2) non-linear power modulation by exploiting the characteristics of power amplifier as explained in [225], or 3) jamming signals to covert the transmitted symbols [226]. This PLE approach focuses on encrypting the data-carrying signals at the physical layer instead of the data itself, and thus preventing Eve from decoding or even sniffing the communicated data packets. In this context, one can see that channel-based key generation schemes may not be considered a complete physical layer security approach as the extracted key is usually applied at the upper layers just like the conventional encryption schemes, making it easy to hack and crack using brute force attacks. Similarly, physical layer encryption schemes may not also be considered a full physical layer security approach due to assuming an already shared keys between communication parities, making it face the conventional problem of key distribution and management. Therefore, it is very useful and meaningful to merge and combine these two approaches together in order to enhance the physical secrecy from one side while avoiding the key distribution problem from the other side. An example from the literature on this combination (although it is not mentioned by the authors) is the work introduced in [227], where the RSSI values are used to extract random sequences that are utilized to rotate the symbols at the physical layer level. Another recent

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2018.2878035, IEEE Communications Surveys & Tutorials

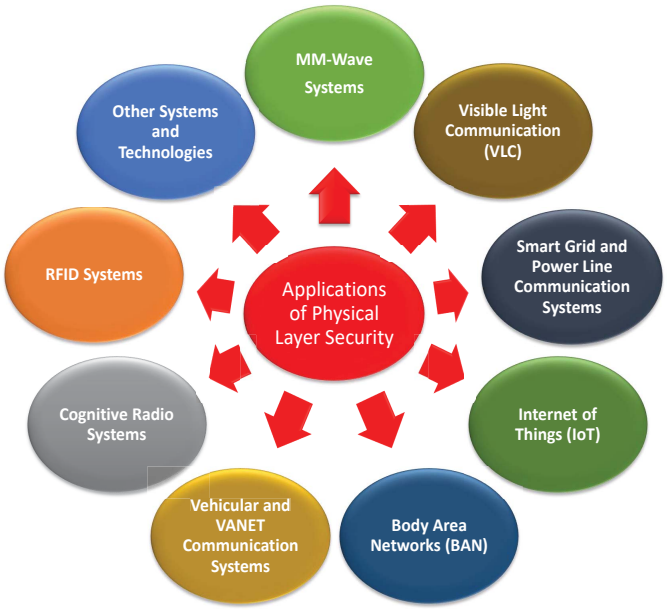

Fig. 16. Main applications of physical layer security to different systems and technologies.

example can be found in [228], where the authors utilized the CSI of massive MIMO system as a key for encryption at the physical layer.

V. Applications of Physical Layer Security

In spite of the fact that many research efforts have been conducted to analyze, characterize, investigate and develop new PLS techniques, most of these works have merely been concentrated on traditional and classical wireless scenarios. However, due to the special characteristics, requirements and features of many other important, emerging communication technologies and systems, new efforts and studies have started accounting and considering PLS for these special systems, such as VLC, smart grid, PLC, IoT, BAN, RFID, vehicular Ad-hoc, cognitive radio, UAV, UWB, D2D, RFID, index modulation, NOMA and mm-Wave technologies. In this section, we present a comprehensive review of the state of the art on applying PLS to these new types of communication scenarios.

It should be emphasized that there are generally three main factors that affect the adoption of PLS in any communication technology. These factors can be summarized as below: 1) the channel characteristics of the considered system or scenario, 2) the capabilities and structure of the transceiver design, and 3) the system requirements needed to meet a certain satisfactory performance level for a specific service or application.

A. 5G mm-Wave Systems

The adoption of PLS in millimeter-Wave (mm-Wave)[10] communication systems is a noticeably emerging area of research. This is motivated by the fact that the characteristics and features of the mm-Wave channel are different from that of micro-wave channel (u-Wave). Consequently, the unique and special features and characteristics of mm-Wave channel including larger system bandwidth, very short wave length, directionality by using massive antenna arrays, and short range transmissions due to severe path-loss propagation, can all together be judiciously exploited to further enhance the secrecy performance of future wireless networks (5G and beyond).

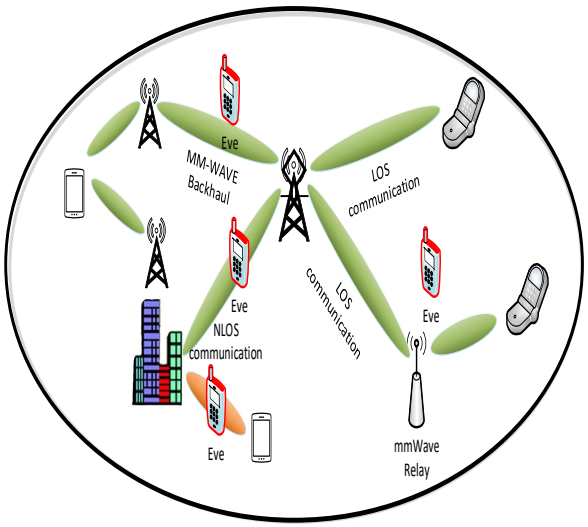

Fig. 17. The application scenario of physical layer security in mm-Wave communication systems.

Many contributions have been made in this domain, here we summarize some of the key works and studies in order to 1) highlight the potential of this new emerging area for boosting and improving the delivered secrecy and 2) to discover and figure out the potential future research topics that can be pursued further. The basic model of PLS for mm-Wave based communication is presented in Fig. 17.

In [229], a detailed secrecy performance analysis of both noise-limited and AN assisted mm-Wave cellular networks using the stochastic geometry framework, and for both non-colluding and colluding eavesdroppers' scenarios was conducted. In [230], the characterization of the secrecy outage considering blockages at Bob and Eve was evaluated in a mm-Wave network coexisted with a microwave network.

In [231], [232], authors explained how to apply the AN-based scheme to mm-Wave systems, and then analyzed the obtained secrecy performance. In [233], three secure transmission schemes were comprehensively investigated over mm-Wave channel by evaluating both the secrecy outage probability and the secrecy throughput. Particularly, the authors analyzed the new secrecy properties of the maximum ratio transmission (MRT) for the mm-Wave system. Then, another two secure transmission schemes were introduced, namely AN-based beamforming and partial MRT-based (PMRT) beamforming.

In [105], a simple directional modulation technique, called antenna subset modulation (ASM), was introduced by utilizing

[10]For having a more detailed background information about millimeter-Wave (mm-Wave) wireless communication systems, we refer the reader to [384].

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2018.2878035, IEEE Communications Surveys & Tutorials

TABLE XVI
AN OVERVIEW OF THE STUDIES ON THE APPLICATIONS OF PLS TO DIFFERENT AREAS OF COMMUNICATIONS

Different types of communication systems	Related references (studies)
5G mm-Wave	[229], [230], [231], [232], [233], [105], [234], [235], [236], [237], [238], [239] [240], [241], [242], [243], [244].
5G Non-Orthogonal-Multiple-Access (NOMA)	[245], [246], [247], [248], [249], [250], [251], [252], [253], [254], [255].
Index Modulation Based Systems	[256], [257], [258], [259], [260], [261], [262], [263], [264], [265], [266], [267].
Visible Light Communication (VLC)	[268], [269], [270], [271], [272], [273], [274], [275], [276], [277], [278], [279], [280], [281], [282], [283], [284], [285], [286], [287], [288], [289], [290], [291].
Smart Grid and Power Line Communication (PLC)	[292], [293], [294], [295], [296], [297], [298], [299], [300].
Internet of Things (IoT)	[301], [302], [303], [304], [305], [306], [307], [308].
Body Area Networks (BAN) and In-Vivo	[309], [310], [311], [312], [313], [314], [315], [316], [317], [318], [319], [320].
Vehicular and VANET	[321], [322], [323], [324], [325], [326], [305].
Cognitive Radio (CR)	[327], [328], [329], [330], [331], [332], [333], [334], [335], [336], [337], [338], [339], [340], [341], [341], [342], [343], [344], [345], [346].
Radio-Frequency Identification (RFID)	[347], [348], [349], [350], [351].
Ultra-Wideband (UWB)	[352], [353], [354], [355], [356], [357].
Device-to-Device (D2D)	[358], [359], [360], [361], [362], [363], [364], [365], [366], [367], [368], [369], [370], [371], [372], [373], [374], [375], [376], [377], [378], [379], [380].
Unmanned Aerial Vehicle (UAV)	[381], [382], [383].

the potential of massive antenna arrays to provide secrecy. It was revealed that ASM achieves coherent symbol detection at the desired direction, while ensuring a high error rate in the undesired directions. In [234], the secrecy throughputs was analyzed from the perspectives of delay-tolerant and delay-limited transmission schemes, using analog beamforming with phase shifters to reduce the system cost. The authors of [235] proposed a new wireless transmission technique, called Silent Antenna Hopping (SAH) or Low complexity ASM [236], to further enhance the achievable secrecy. SAH is composed of a phased-array transmitter followed by antennas with an on-off switching circuit. This scheme ensures scrambling the constellation points in both amplitude and phase in the undesired directions, while maintaining a clear constellation in the intended direction.

In [237], the authors generalized the scheme proposed in [235], [236] to a new architecture, called switched phased-array (SPA), to further enhance the physical security. SPA was shown to work as a platform for three different transmission techniques: 1) conventional phased-array transmission; 2) antenna subset transmission (AST) technique; and 3) silent antenna hopping (SAH) transmission technique. In [238], the authors proposed a transmission scheme which can provide more security than the ASM scheme proposed in [105] and with low computational complexity. This was attained by designing an optimized antenna subset selection based on an iterative fast Fourier transform (FFT). The physical layer security performance in mm-Wave ad-hoc networks was explored in [239], where eavesdroppers are randomly located, and can intercept the confidential messages as they may be situated in the main signal beam. Particularly, the authors characterized the impact of mm-Wave channel features, random blockages, and antenna gains on the secrecy performance.

In [243], the authors throughly studied physical layer security in a MISO mm-Wave scenario in which multiple eavesdroppers with single-antenna are randomly situated in the network. In this study, both maximum ratio transmitting (MRT) beamforming and artificial noise (AN) beamforming are investigated. It is reported that the achievable secrecy level is closely affected by eavesdroppers' density in the network as well as the spatially resolvable paths of both Bob's and Eve's channels in mm-Wave system. The work in [385] studied secure beamforming (BF) for fifth generation (5G) cellular system operating at millimeter wave (mmWave) frequency and coexisting with a satellite network. In this work, a uniform planar array is employed at the base-station where it is assumed that the channel state information of multiple eavesdroppers based on imperfect angle-of arrival (AoA) is known. Under the constraint of the interference and transmit power of BS, authors formulated a constrained optimization problem in order to maximize the secrecy rate of worst case of the cellular user. Afterwards, they also proposed two beamforming methods to solve the optimization problems for the case of uncoordinated and coordinated Eves. In [386], the authors proposed an interesting PLS scheme for mm-wave communication based on a hybrid MIMO phased array time modulated DM. The basic idea is to divide the transmit array into multiple sub-arrays. All the sub-arrays can jointly work as a MIMO for multi-user communications or higher angular resolution while each sub-array forms a secure directional beam. More importantly, effective security can be achieved by applying a time-modulated DM scheme for phased MIMO mm-wave wireless communication without having knowledge of eavesdroppers.

As it can be seen from the above literature, many of the proposed approaches for securing mm-Wave systems do not pay much attention to the fact that applying security techniques in the digital baseband domain (similar to conventional systems) is extremely challenging in mm-Wave and should be avoided as much as possible due to issues related to power, complexity and cost. Therefore, there is a need for devising new practical security designs that can be implemented in the analog domain instead of using purely digital domain-based schemes. Recently, there have been some emerging studies on hybrid analog-digital designs for physical layer security in mm-Wave as can be found in [240]–[242].

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2018.2878035, IEEE Communications Surveys & Tutorials

B. 5G Non-Orthogonal-Multiple-Access (NOMA)

Recently, there has been an increasing interest in NOMA[11] due to its ability to provide low latency, improved coverage, massive connectivity and high reliability for 5G and beyond wireless network. Due to these uniques properties it has been recognized as one of the most significant enabling technology for 5G and beyond. Thus, design and implementation of PLS techniques for NOMA technology is one of top priority. The basic system model for NOMA-based networks for PLS is presented in Fig. 18. Unlike point to point communication scenarios, in NOMA schemes, there are two kinds of eavesdroppers: one is external passive eavesdropper, whose channel cannot be known at the transmitter, and another internal active eavesdropper (i.e., normal user), whose channel can be known at the transmitter. Therefore, the objectives of the security design in NOMA can be divided into two major tasks: 1) security against external eavesdroppers and 2) security against internal eavesdroppers.

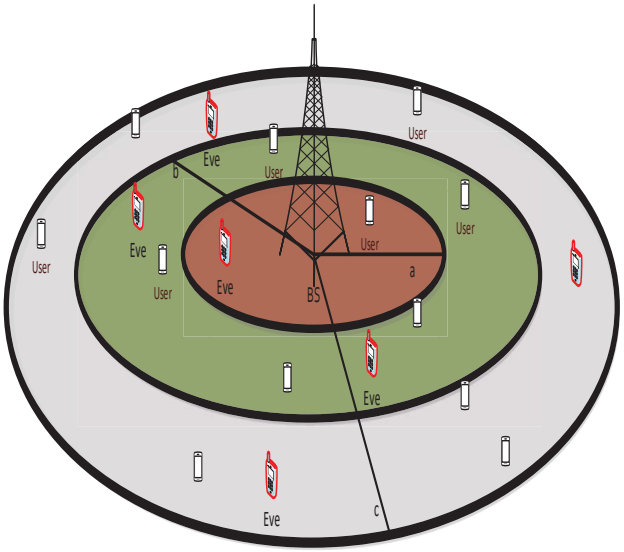

Fig. 18. Physical layer security scenario for NOMA.

For the external eavesdropper case, the primary goal is to utilize NOMA transmission structure and modify it in such a way that makes it more robust against external eavesdropping problem. The main approaches used in the literature to mitigate the aforementioned security problems are to find the optimal power allocation policy and beamforming strategy that maximize the secrecy sum rate, while satisfying the QoS requirements of each user. This includes optimizing the transmission rates, the power allocated to each user, the channel ordering of the NOMA users alongside their decoding order, and trying to add interfering signals to help enhance the secrecy performance level.

For the internal active eavesdropper case, the main security concern is stemmed from the fact that each user has to decode other users' signals before he is able to decode his own signal using successive interference cancellation (SIC) process. As inferred, the goal here is to protect the transmission not only from the external eavesdroppers, but also from the other internal multiplexed users (which seems to be a very challenging practical task).

Here, we survey the key contributions on the direction of applying PLS to NOMA-based systems. In [245], the authors studied for the first time in the literature the application of PLS to downlink SISO-NOMA scenario and formulated the problem of finding the optimal power allocation policy that maximizes the secrecy sum rate against external eavesdropper given a certain constraint on the QoS requirements of each user in the network. It was shown that the secrecy rate provided by NOMA significantly outperforms that delivered by conventional orthogonal multiple access (OMA).

In [246], the authors considered the secure transmission of a downlink MISO-NOMA scenario, where the multiplexed users are divided into multiple groups, each consists of a cell-central (near) user and a cell-edge (far) user. The near user is considered to be an intended legitimate user, whereas the far user is a potential internal eavesdropper. The authors studied the joint optimization of both beamforming and power allocation design that maximizes the sum secrecy rate of near user subject to a certain transmit power constraint at the transmitter and target rate requirements at near users. A challenging yet practical and interesting scenario would be to consider the near user (instead of the far one) to be the potential eavesdropper and see what security technique would be useful to secure such a scenario and how much would be the obtained security performance level.

In [247], the secrecy sum rate maximization problem for a downlink MIMO-NOMA system that consists of a base station, multiple legitimate users, and an external eavesdropper was investigated. For the same scenario (i.e., MIMO-NOMA), the authors in [248] considered a scenario similar to that adopted in [246]. The authors addressed the problem of internal far user eavesdropping the communication of near cell-edge users by designing an optimized secure beamforming scheme to maximize the secrecy rate subject to a certain transmit power level and a data rate target. In [249], the PLS of NOMA in large-scale networks was investigated by using stochastic geometry, where both single-antenna and multiple-antenna base station scenarios are considered. In the case of single-antenna-aided base station (BS) scenario, a secure area around the BS is adopted to provide an eavesdropping-free zone with the help of judicious channel ordering of the multiplexed users. For the case of multiple-antenna-equipped BS scenario, artificial noise is produced at the BS to further enhance the secrecy level.

In [250], the authors considered the application of NOMA with mixed multicasting and unicasting transmission cases to improve the spectral efficiency as well as secrecy. The proposed joint beamforming and power allocation design guarantees improving the unicasting performance while preserving the reliability of multicasting.

In [251], a new secure NOMA design was introduced to protect the transmission against external passive eavesdroppers. The optimal designs of data rates, decoding order, and power

[11]For acquiring a deeper background information about non-orthogonal-multiple-access (NOMA) systems, we refer the reader to [387].

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2018.2878035, IEEE Communications Surveys & Tutorials

assigned to each user are inspected and investigated, where the secrecy outage probability was adopted as the secrecy metric. The problem of minimizing the transmit power subject to the secrecy outage and QoS constraints was first formulated, and then a closed-form solution to this problem was derived. Furthermore, the problem of maximizing the secrecy rate among users (motivated by the need to provide fairness among users) subject to the constraints of certain secrecy outage and transmit power was also studied, where an iterative algorithm was provided to solve this problem.

In [252], the authors investigated the secrecy performance of a two-user downlink NOMA systems, where both SISO and MISO scenarios with various transmit antenna selection (TAS) strategies are considered. Exact closed-form formulas for the secrecy outage probability with suboptimal TAS and optimal TAS schemes are obtained and compared with the conventional space-time transmission scheme. Moreover, a power allocation scheme is suggested to achieve non-zero diversity order with all the TAS schemes.

In [253], motivated by the fact that internal eavesdropping may appear between the users in NOMA. The authors advocated that although existing PLS schemes can be used to resist eavesdropping, good eavesdropping-resilient schemes in NOMA should account for the following three rules: (1) successive interference cancellation (SIC) should be operated without imposing any further extra processing; (2) each user can not obtain other users' information; (3) the adopted scheme is preferable to be independent of the spatial contrast between channels due their possible high correlation. Motivated by these rules, the authors proposed a new security scheme that can abide by these rules. In the authors' scheme, the original information signals of users are transformed into the signals to be transmitted using a specially designed angle conversion process, where the principles and details of these variations are different for various users. Furthermore, a conducive mechanism with full-duplex technology is developed to guarantee that the users can learn the principles safely. By this scheme, each user can deduce other users' transmitted signals to operate SIC normally, while the original signals are difficult to be determined from transmitted signals and can only be obtained by the corresponding legitimate users.

In [254], the authors investigated the PLS of NOMA with both Half Duplex Relay (HDR) and Full Duplex Relay (FDR), where one external eavesdropper and two legitimate NOMA users are considered with the assumption that far user is getting assistance from a dedicated FDR or HDR.

In [255], the problem of secure transmission in untrusted relay networks was studied. Unlike conventional orthogonal relaying, a new non-orthogonal relaying scheme is devised to maximize the secrecy rate. Particularly, the source and relay nodes are allowed to transmit signals concurrently over non-orthogonal channels (which causes co-channel interference), and successive interference cancellation is normally applied at the destination node to decode its corresponding signal. The authors also proposed two transmit antenna selection schemes to further enhance the security. In [388], authors proposed PLS technique for 5G wireless networks with massive connections in the presence of multiple active eavesdroppers. In order to realize secure communication, NOMA and non-orthogonal channel estimation (NOCE) are combined to enhance the signal quality at the legitimate user only. In order to deliberately confuse the eavesdroppers, inter-user interference is harnessed without exploiting AN. Moreover, the authors also proposed that the transmit power should be optimized during multiple access stage and channel estimation stage in order to fully exploit the inter-use interference for security enhancement.

As it can be inferred from the above literature, to safeguard the transmission of 5G and beyond networks, the PLS has been applied to NOMA and used with different scenarios such as SISO, MISO, MIMO, large-scale networks, relays, etc. Particularly, techniques such as optimal power allocation, beamforming optimization, and transmit antenna selection are examples of potential techniques that can be used to improve the secrecy of NOMA transmission. Thus, it is foreseen that the research area of applying PLS to NOMA will expand to cover other scenarios of interest such as NOMA with STBC, spatial modulation (index modulation or space shift keying), cooperative transmission with relays of all types, cooperative multiple point, cognitive radio including both underlay and overlay, full-duplex, etc.

C. Index Modulation Based Systems

Index modulation is a new emerging type of modulation [389] that enhances power efficiency and reliability. It aims at sending part of the data bits (besides the bits sent by conventional constellation-based modulation) by changing the indices of transmit resources that can be available in space (antenna), frequency (subcarriers), or time (slots) according to the different possible combinations of the incoming data bits from the source. This has been motivated by the fact that index modulation performs better than that of conventional constellation-based modulation in terms of energy efficiency, reliability, and robustness against inter-channel-interference (ICI) problem while providing flexibility in the delivered data rates. Generally speaking, applying index modulation concept in spatial domain results in what is commonly called as spatial modulation (SM), where both antenna index and ordinary signal constellation modulations are used to convey information. Also, when only antenna index is used to send information, the resulting transmission scheme is termed in the literature as space shift keying (SSK). On the other hand, applying the same concept in the spectral domain of OFDM signal results in what is called as subcarrier index modulation (SIM) or what has commonly become well-known as index modulation (IM)[12].

Due to the inherent differences between index and classical data symbol modulation as the detection of active antennas in case of MIMO-SM or active subcarriers in case of OFDM-IM is different from the classical detection of data symbols in signal constellation, many of the existing PLS may not be directly applicable and new index modulation-tailored PLS techniques need to be designed for securing the data sent by the indices of the transmit resources. In this section, we review

[12]For a more comprehensive understanding of the area of index modualtion, we refer the reader to [390].

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2018.2878035, IEEE Communications Surveys & Tutorials

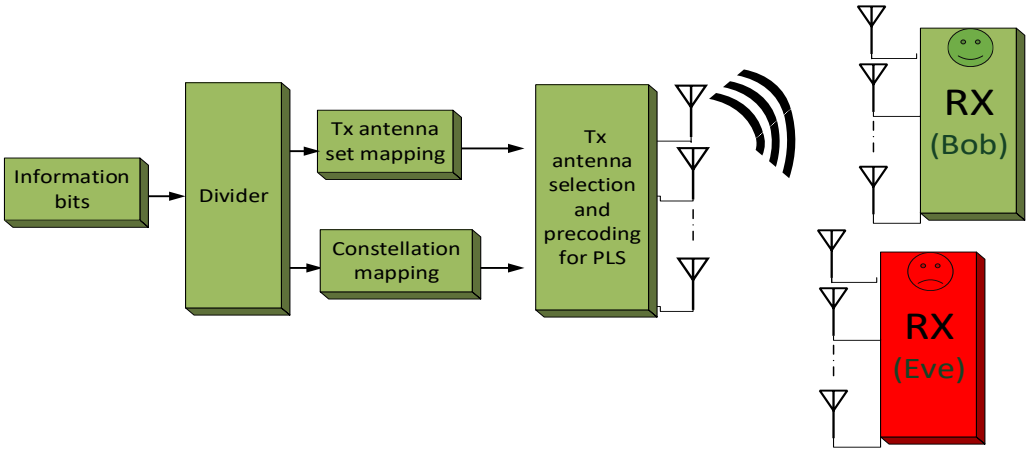

Fig. 19. Physical layer security scenario for spatial modulation systems.

some of the key advances and recent studies on applying PLS concepts for index modulation schemes. The basic system model of applying PLS to index modulation in space domain (i.e., spatial modulation) is shown in Fig. 19.

In [256], Sinanovic *et al.* studied and investigated for the first time in the literature the secrecy capacity performance of both SM and SSK in the context of wireless security systems. It was shown that the effect of constellation size depends on the SNR values of Bob and Eve. For low Eve's SNR, smaller constellations have better secrecy than larger ones over all SNR values, while for the high Eve's SNR, larger constellations gives larger secrecy capacities. Also, it was noticed that the secrecy capacity of SSK is worse than that of the spatial component of SM at high SNR. In [257], the secrecy capacity of SM with finite input alphabets is derived, and then a precoding scheme (that considers the CSI of Eve available at Alice) is introduced to improve the secrecy performance of SM.

In [258], the authors extended the study of [256] by deriving generic secrecy capacity expressions that enable calculating the achievable secrecy rates for both SSK and SM. Particularity, they investigated the effects of increasing antennas' number at Alice, Bob and Eve on the secrecy behavior of SSK. In addition, the achievable secrecy rates of SM were evaluated with different signal constellations and then compared with those of ordinary MIMO systems. It was concluded that SM achieves higher secrecy rates than the traditional SISO schemes, but lower than that of general MIMO systems. In [259], the authors studied the effectiveness of SM transmission along with jamming without knowing Eve's channel. They showed that the secrecy performance and transmission power trade-off in jamming by presenting new results on the achievable secrecy rate and BER at different receivers.

In [260], the effect of knowing channel state information at Alice on the achievable secrecy rates of SSK was investigated. A new iterative algorithm was formulated to optimize the achievable secrecy rates. Also, two low complexity precoding algorithms were proposed for different setups based on the number of antennas at Eve to attain positive secrecy rates over any SNR value. In [261], the authors exploited the channel reciprocity of TDD systems to design a secure SSK scheme, where the indices of the transmit antennas are allocated dynamically based on Alice-to-Bob channel that is naturally different from that of Alice-to-Eve. Also, the effects of imperfect channel reciprocity and existence of a nearby Eve on the reliability and eavesdropping immunity of the proposed scheme were studied. To enhance secrecy against nearby eavesdropping and robustness against imperfect reciprocity, antenna index assignment algorithm was proposed. In [262], the authors exploited the precoder design used in precoding-aided spatial modulation (PSM), which partially sends information by the receive antennas' indices, to provide secure communications. Particularly, the precoder structure was deliberately optimized to jointly minimize the SNR at Eve (assuming the knowledge of Eve's channel) while maximizing it at Bob. The conducted performance analysis in terms of error and ergodic secrecy rates showed that positive secrecy along with low-complexity detection can concurrently be attained at Bob even for the cases when Eve utilizes more receive antennas than the desired receiver. In [263], the PSM was generalized to an eavesdropping-resilient secret PSM (SPSM) scheme without assuming the knowledge of Eve's channel at Alice. Particularity, a time-varying precoder structure was designed in order to keep all the merits of PSM at Bob while generating time-varying interference at Eve. The scheme was demonstrated to provide secrecy even for the cases when the number of antennas at Eve is higher than that of Bob.

In [264] the precoding-aided spatial modulation (PSM) was generalized to a multiuser (MU) downlink scenario where the proposed scheme named as MU-PSM was shown to be immune against multiple antenna eavesdropper. Particularly, precoding matrices are intended to eliminate the inter-user-interference and modulate partial bits on the indices of receiving antennas. To further enhance the security, scrambling of precoding matrices is designed to cause a fast-varying precoding matrix, which results in more degradation at Eve even if she uses blind estimation and detection. In [265], the authors proposed a PLS scheme that redefines the transmit

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2018.2878035, IEEE Communications Surveys & Tutorials

antennas' indices by exploiting the channel reciprocity of TDD systems and knowledge of the legitimate CSI between Alice and Bob. Due to channel reciprocity, only Bob can detect the spatial bits, while Eve is kept unable to do so as she does not have the legitimate CSI. However, in this scheme the information bits sent by signal constellation is not secure. Due to this particular deficiency, in [391], the authors introduced a secrecy enhancement scheme for SM systems, where both the indices of transmit antennas and constellation symbols are rotated with the knowledge of the legitimate CSI between Alice and Bob to prevent Eve from detecting any information bits transmitted via both indices and constellation symbols.

In [266], a full-duplex receiver aided secure spatial modulation (FDR-SSM) scheme was proposed, where secrecy is improved by sending jamming signals from a full-duplex legitimate receiver that can cancel its own generated jamming signals while causing severe time-varying interference at Eve. In [392], authors proposed a novel physical layer technique for the exchange of secret key and authentication based on random constellation mapping in spatial modulation systems. More specifically, the authors used the basic symbol-antenna mapping feature in SM and applied channel based approach to impose a random phase shift on each symbol for key exchange and authentication. An effective PLS technique for SM systems was proposed in [393] and referred to as mapping-varied spatial modulation. In this technique, the transmitter varies the antenna information of SM and mapping patterns for the radiated information based on the instantaneous pattern of Bob's channel quality. Due to channel decorrelation, Eve cannot decode the confidential information. The authors also presented the derivations related to the secrecy rate, ergodic secrecy rate, and secrecy outage probability.

Moving from MIMO-SM to OFDM-IM, one can find out that the first and only study so far on applying PLS to OFDM-IM has recently been introduced in [267], where the authors investigated channel-based randomized mapping rules for securing index modulation alongside data symbol modulation. Due to these mapping rules related to data symbol and index modulation in OFDM-IM, Eve cannot decide about message bits correctly (i.e., she cannot decode), even though she can detect and estimate the active subcarriers and their corresponding symbols correctly. This scheme is somehow similar to physical layer encryption approach where the shared channel knowledge is used to randomize the modulation mapping rules, which belong to the properties and functionalities of the lower physical layer.

As noticed from the above-reviewed literature, many PLS research studies and works have been focusing on MIMO-SM and MIMO-SSK, but extremely very little amount of works exists on studying the PLS of OFDM-IM. So, a natural direction is to gear some of our efforts as researchers towards designing and developing new effective security techniques for OFDM-IM. In other words, it is meaningful to give enough attention to the PLS of OFDM-IM in a comparable level to that given to MIMO-SM.

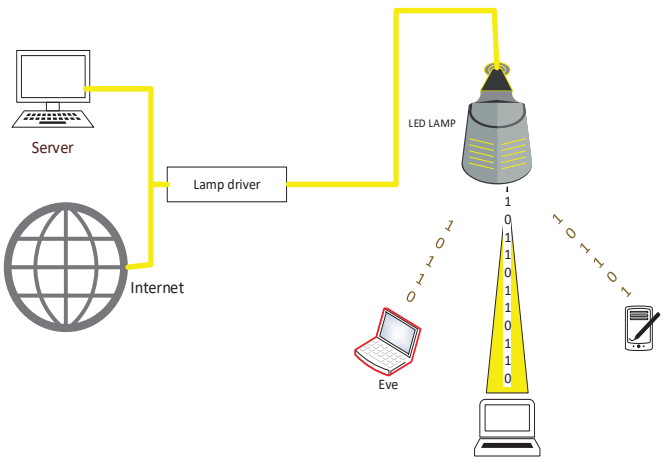

Fig. 20. Physical layer security of a generic VLC scenario in the presence of an eavesdropper.

D. Visible Light Communication (VLC)

Visible light communication (VLC)[13] channels have their own unique characteristics which are different from RF ones. One prominent difference is that VLC signals cannot penetrate human and normal building blockages, making its communication inherently secure from the outdoor eavesdroppers. However, the inherent eavesdropping resilience feature of VLC signals cannot hold in the cases of public areas or multiple-user indoor scenarios. To confront this limitation, physical layer security of VLC scenarios as visualized in Fig. 20 has recently been considered. Studying the physical-layer security of the visible light communication (VLC) channel and evaluating its achievable secrecy performance was first performed by Mostafa *et al.* in [268]. In their work, artificial noise and null-steering strategies were utilized to attain positive secrecy rates for the cases of both SISO and MISO and when Eve's CSI is initially present and then absent at the transmitter [268], [269]. In [270], massive two-dimensional LED array was exploited to boost the secrecy of VLC links. Specifically, the excessive spatial degree of freedom provided by the massive LEDs was utilized to enhance the secrecy rate without having accurate knowledge about Eve's location.

In [271], the authors considered MIMO-VLC scenario, and introduced an approach based on data beamforming for providing secrecy. In [272], the VLC-based PLS was extended to include friendly jamming-based schemes, by which the Eve's reception is made contaminated by a jamming signal (artificial noise), while maintaining zero interference to the Bob's channel. In [273], an enhanced achievable secrecy rate of VLC with cooperative jamming was investigated and analyzed considering a peak amplitude constraint on the input distribution. In [274], the secrecy sum-rate in multi-user MISO (MU-MISO) broadcast VLC systems was studied. Particularly, zero-forcing precoder is utilized to achieve secrecy among users. In [275], the design of secure transmit beamformers,

[13]For becoming familiar with the topic of visible light communication (VLC), we refer the reader to [394].

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2018.2878035, IEEE Communications Surveys & Tutorials

in indoor MISO VLC links, that maximize the achievable secrecy rate subject to peak amplitude constraints, was studied. Due to the condition on the amplitude of the input data, the design problem turns out to be non-convex and hard to solve. However, it was shown in [275] that this non-convex optimization problem can be converted into a solvable quasi-convex search problem.

Moreover, in [276], the authors computed the achievable secrecy rate via transmit beamforming and artificial noise in MISO scenario for different input distributions, including the uniform and truncated generalized normal (TGN) distributions. Also, in [277], the optimal beamforming vector, subject to constrained inputs, was derived in closed form when Eve's location is known, whereas a robust beamforming is applied when Eve's position is unknown. In [278], the effect of light reflection and channel path correlation on VLC security was demonstrated. Particularly, a more advanced eavesdropping-resilient framework was presented under both SISO and MISO models. Also, a random time reversal scheme, that focuses the transmitted signal towards the legitimate receiver while interfering the Eve's channel, was designed by making use of the multipath redundancy in VLC channel. In [279], authors designed and analyzed the PLS mechanism with the help of ill-posed theory and exhibited a channel-based sub-carrier shifting scheme with pre-equalization. In [280], a differential chaos-based modulation, with channel scrambling for wavelength-division multiplexing (WDM) aided VLC system, was introduced to enhance the transmission security over red, green, and blue (RGB) channels. The scheme utilizes the diversity property of LED and the inherent high-security feature of chaotic sequences. Also, 3-D multiuser visible light communication (VLC) network was recently studied in [288].

In [395], secret key agreement (generation) was investigated and examined in MISO VLC systems, where upper and lower bounds are obtained. Particularly, a fractional programming-based two-stage approach was exhibited for the secret-key construction. In [281], the confidentiality of VLC systems is enhanced by suggesting a new key extraction protocol for optical OFDM schemes in an indoor environment. The authors introduced a scheme capable of extracting keys from the bipolar OFDM samples resulted from the optical OFDM modulation process [282], [283].

In [289], the secrecy capacity of indoor VLS systems has deeply been analyzed. Particularly, two different scenarios are studied: one is investigated with a constraint on the average optical intensity only, whereas the other is investigated with constraints on both average and peak optical intensity. Similar to work performed in [289], where constraints on the peak and average intensities are considered, the optical VLC wiretap channel with input-dependent Gaussian noise has been studied in [290]. Particularly, it is proven that the input distribution that can achieve the secrecy capacity is discrete with a finite number of mass points, with one of them placed at the origin. In [291], the secrecy outage probability of a multiuser VLC system adopting non-orthogonal multiple accessing scheme has been investigated, where closed-form expressions are provided.

Besides applying PLS for VLC, there is also some recent interest in applying PLS for free space optical (FSO) communication. Examples on studies related to applying PLS to FSO can be found in [284], [285], [286], and [287].

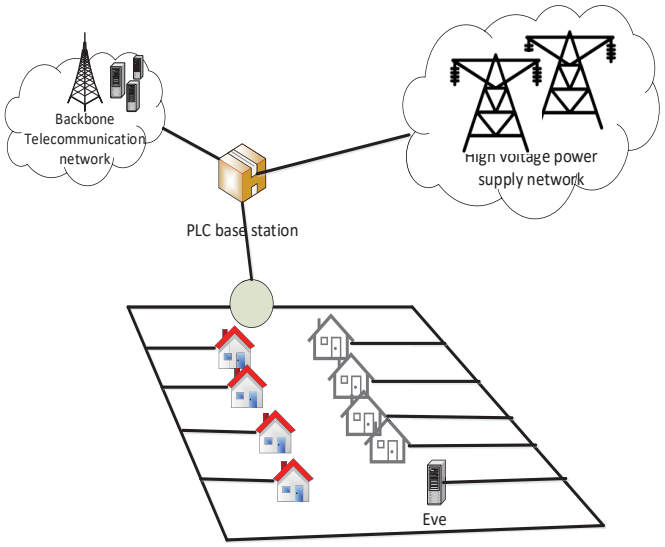

Fig. 21. Power line communication in the presence of eavesdroppers.

E. Smart Grid and Power Line Communication (PLC) Systems

Like many communication systems, smart grid systems[14] are susceptible to eavesdropping problem. The conventional approach to address this challenge and provide secrecy for this kind of systems has been to use cryptographic-based methods. However, due to the special requirements of smart grid networks represented mainly by fast monitoring and controlling, complex encryption-based techniques are deemed unsuitable. Consequently, significant attention has been paid to utilize PLS as an alternative approach that can provide reliable secrecy, while meeting the requirements and constraints of smart grid networks. The basic system model for PLC in the presence of eavesdropper is presented in Fig. 21. In [292], a description of a fast and secure scheme utilizing random spread spectrum concept is provided. Moreover, a technique, called Frequency Quorum Rendezvous, is proposed. In this technique, two random hopping sequences are coordinated using a quorum system and without the need to any pre-shared knowledge among communicating nodes. Later, the PLS concept was directly applied on power line communication (PLC) systems in [293]. In that study, the achievable secrecy rate and the effect of the channel on the performance was thoroughly investigated. This pioneering work was extended in [294] to include calculating the secrecy rate for the multi-user broadcast channel assuming not only simulated channel realizations, but also experimental channel measures. The secrecy capacity of MIMO PLC was evaluated in [295], where it was shown that MIMO structure enhances the secrecy rate of PLC systems. A deep performance investigation using average secrecy capacity

[14]For obtaining more background information about power line communication and smart grid networks, we refer the reader to [396].

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2018.2878035, IEEE Communications Surveys & Tutorials

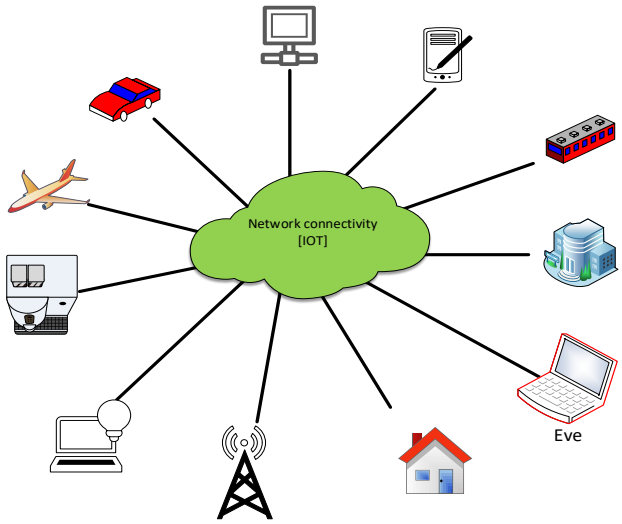

Fig. 22. Various IoT applications under the risk of eavesdropping problem.

for cooperative relaying PLC systems, with artificial noise in the presence of an eavesdropper, was performed in [296].

The authors in [297] found the optimal power allocation sequence for providing security in multicarrier relay power line communication. A recently related and generic work performed on this area was presented in [299], in which a security technique for wire-line point-to-point communication was proposed. In [298], the authors investigated the impact of the wireless PLS and reliability on demand-side management process in the smart grid network. Particularly, they showed, using their proposed artificial noise-aided OFDM scheme, that higher secrecy can be obtained at the expense of reducing reliability. In order to mitigate this trade-off, a new encoding technique, utilizing the degree of freedom provided by non-ideal meters, was proposed in [298]. Recently, MIMO-OFDM transceiver for NB-PLC applications in multi-user medium-voltage multicasting networks has been proposed and then two schemes are developed for securing its data transmission [300]. The first scheme provides security against active eavesdropper whose CSI is known at the transmitter, whereas the second scheme achieves secrecy against external passive eavesdroppers whose channels cannot be known at the transmitter [300].

F. Internet of Things (IoT)

IoT[15] is expected to be an indispensable part of our daily lives, where different applications and various use cases served by IoT infrastructure can be susceptible to the eavesdropping problem due to their wireless connectivity as shown in Fig.22. Due to some special constraints on the size, power, and computational complexity of IoT devices alongside the unique properties of their uplink and downlink communication represented by low signaling overhead and sporadic low data traffic, many of the current existing physical layer security techniques are deemed inefficient, unsuitable, and not easy to implement for IoT devices. The reasons behind this barrier lie on the unique requirements of IoT systems which can be summarized as follows:

- In the uplink of the IoT system, which is usually composed of sensors collecting and sending data to a legitimate fusion center (controller or access point) as shown in Fig.23, each one of the transmit sensors is normally equipped with only one antenna due to their compact size, low complexity, and low data rate requirements. Thus, the degree of freedom in space domain which normally comes with multiple antenna utilization is no longer available. Consequently, MIMO-based security techniques may no longer be used in such a scenario [20], [301].
- In IoT networks, continuous channel sounding and full, precise acquisition of the legitimate channel state information at the transmitter (CSIT) is prohibited due to the fact that the number of channel training opportunities is limited and high-rate feedback channel is forbidden to avoid signaling overhead. In fact, sending training pilots frequently for channel estimation is power inefficient and also it sacrifices too much spectral resources in the case of dense IoT deployment scenarios. Therefore, secret key generation methods from the reciprocal legitimate channel are no longer applicable, especially if there is also no much channel randomness as is the case in flat fading channels with less selectivity in time and frequency domains.
- Since eavesdroppers are external to the IoT network and remain completely passive, nor their locations neither their CSIT can be known at the transmitter as it is almost impossible and extremely hard to acquire them in reality. This means that Eve might have a channel quality as good as or even better than the legitimate receiver. Thus, many security methods that rely on these assumptions will practically fail to fulfill the confidentiality requirement. An example of these methods is security channel coding schemes, which normally consider that Eve's channel is a degraded version of the legitimate channel.
- On the contrary to the uplink, the downlink of an IoT system is usually composed of a legitimate fusion center controller sending command data to actuators as shown in Fig.23, each one of the controllers can be actually equipped with multiple-antenna due to their relatively high computational power and extra capabilities, while each actuator is equipped with one antenna due their limited complexity and computational power resources as well as their compact size. Therefore, the security schemes that can be applicable in the uplink case might become no longer suitable in the downlink and vice-versa due to the difference in the requirements and capabilities of the transmit side.

These special requirements motivate developing new security schemes tailored to IoT applications. Thus, several recent works have focused on re-visiting and rethinking physical layer security from the IoT requirements perspective [301]–[304]. Particularly, authors in [301] offered a comprehensive

[15]For obtaining more background information about Internet-of-Things (IoT), we refer the reader to [397], [398].

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2018.2878035, IEEE Communications Surveys & Tutorials

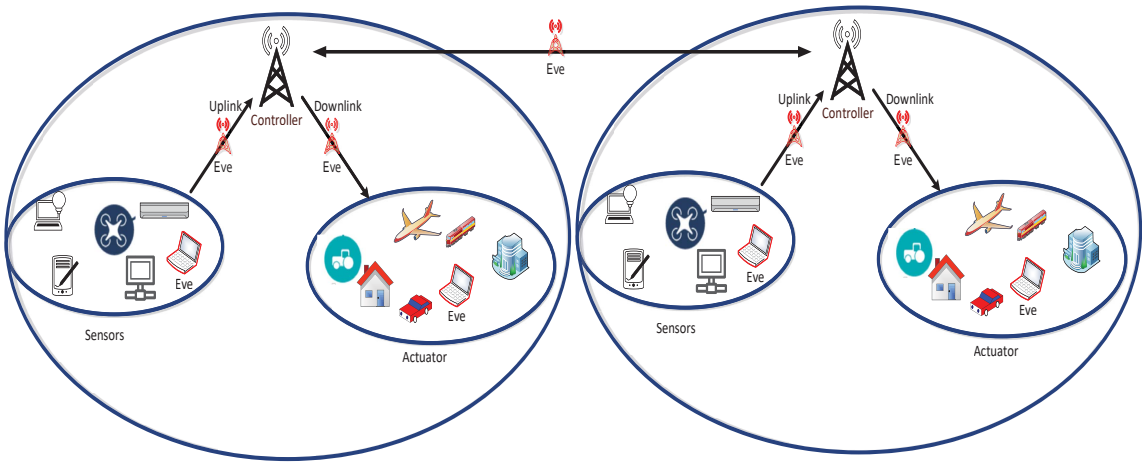

Fig. 23. Basic Internet of Things (IoT) system composed of both uplink (sensor to controller) and downlink (controller to actuator) communication.

review of current state of the art and challenges in security schemes that are deemed to be convenient for IoT applications. These candidate secure IoT techniques along with their concepts, advantages and drawbacks are reviewed and summarized in TABLE. XVII. In addition, the authors in [307] proposed and implemented a technique that utilizes the physical layer security concept to set up a secure channel that facilitates the exchange of confidential keys between legitimate IoT devices, resulting in an improved secret key exchange protocol while assuring low management and communication overheads. In [308], the authors introduced a compressed sensing-based security model, where a circulant matrix is utilized as a measurement matrix in order to enhance the efficiency of the key generation process. The effectiveness of the scheme was validated and verified by practical and experimental implementation using IoT hardware devices.

G. Body Area Networks (BAN) and In-Vivo Systems

The security issue of wireless body area networks (BAN)[16] and implantable medical devices (IMD) as pictured in Fig.24 is a growing area of research. BAN consists of actuators, sinks and sensors that are small sized, lightweight, ultra-low-power and intelligent units. These small units are placed at various specific location inside and on the body and thus enable us to continuously monitor, analyze and treat different health issues. IMD are special units that are part of BAN and can be placed inside the body, i.e cardiac pacemakers, neuron stimulator, etc. and also can be programmed wirelessly to carry out different functions, for example, data extraction and parameter configuration [309]. The use of wireless technology makes BAN extremely vulnerable to eavesdropping, jamming and spoofing attacks; that may lead to serious issues, such as mistreatment, theft of critical information and may even cause death in extreme cases [309]. One of the key challenges in BAN field is to protect these devices from eavesdropping because unauthorized users can learn sensitive information by eavesdropping to carry out various attacks.

[16]For obtaining more background information about Body Area Networks (BAN), we refer the reader to [399].

Candidate Secure IoT Technique	Concept	Advantages	Drawbacks
Channel Aware Encryption (CAE)	Data manipulation based on the instantaneous channel fading gain of the legitimate receiver.	Low complexity and coarse partial CSI (only the channel amplitude).	Bandwidth penalty is caused due to the use of channel two times to send one bit.
Optimized ON–OFF Switching	A threshold is selected by the Tx to determine whether to transmit to a certain receiver at a given time period.	Moderate complexity and high energy efficiency.	The scheme requires knowledge of the SINR and the statistical distribution of eavesdropper channel.
Noncoherent Communication Schemes	Achieving secrecy through exploiting the statistical CSI instead of the instantaneous one.	Simple implementation and no need for instantaneous channel knowledge.	Not knowing the instantaneous CSIT of the legitimate channel may lead to a zero secrecy rate as the transmission rate cannot be set precisely.
Secure Space-Time Coding	Selecting the best precoding matrix from a codebook of matrices that maximizes the SNR at the legitimate Rx.	Moderate CSI requirements with high energy efficiency.	Relatively complex and cannot ensure perfect secrecy at any SNR Eve may have.
Artificial Noise	Injecting an interfering signal in the null space of the legitimate receiver to degrade Eve's SNR.	Can achieve perfect secrecy and also applicable when Eve is closer to the BS than other users.	Applicable only when the number of antennas at the transmitter is more than that at the legitimate receiver and eavesdropper; low energy efficiency.

TABLE XVII
CANDIDATE SECURE IOT TECHNIQUES.

The security for BAN is challenging because of some units in BAN, i.e. IMDs are resource-constrained, reduced-size, light-weight, requiring low duty cycle with low peak power. Due to this, the security techniques for BAN should be computationally simple, power efficient and effective. Another unique challenge in IMD security design is accessibility versus security, which means that security techniques should provide access to unauthorized users in case of emergency via some specific protocols, i.e access to IMD of unconscious patient in case of emergency to unauthorized doctor [310] [311]. Based

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2018.2878035, IEEE Communications Surveys & Tutorials

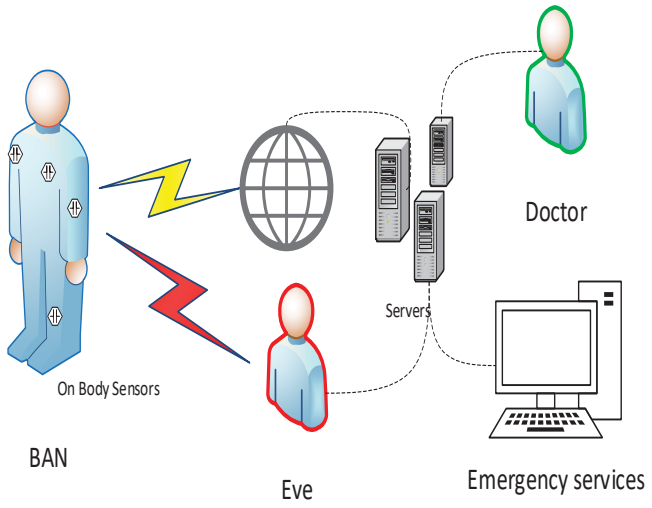

Fig. 24. Basic BAN system model under eavesdropping problem.

on these requirements, many security techniques have been proposed in the literature where the majority of them focus on using cryptographic based-approaches. Aside from crypto-based techniques, many PLS approaches for BAN have been introduced in the literature.

In [312], a jamming based technique, called ally friendly jamming, was proposed to protect transmission against eavesdropping. The technique enables the legitimate receiver to recover the transmitted signal successfully while the eavesdropper is kept disable from decoding the transmitted signal. The only problem with this technique is that it cannot work in the presence of malicious jammers. In [313], another external device assisted PLS method against eavesdropping was presented. The device, called as shield, works as a relaying device between the external programmer and IMD in such a way that it receives the signal from IMDs and jams them at the same time to avoid eavesdropping from an unauthorized devices. It then applies encryption to the message received from IMD and sends it to legitimate programmer. All the commands from external programmer must be sent to shield first, and then relays the valid commands to IMD. The shield also jams any command that is directly sent to IMD, thus saving it from any unauthorized misuse. In [314], the authors analyzed the application of multi-hop relaying for the improvement of PLS in BAN. The authors showed that secrecy outage performance (SOP) of multi-hop outperforms single-hop's SOP. The reason for this is that there is a severe path loss in case of human body. In [315], a security technique to secure data provenance for body-worn devices using spatial and temporal characteristics of wireless channel was introduced. The solution enables the legitimate parties to generate correlated fingerprints. These fingerprints associate a data session uniquely with a wireless link, which are very hard for an eavesdropper to forge. The authors validated their technique with experiments. The author also optimized the results with respect to resource constraints.

In [316], an RSS based energy efficient key generation method was proposed for BAN. In this technique, channel sampling is applied during routine transmission instead of dedicated communication; and in order to mitigate noise component a Savitzky-Golay low pass filter is applied. Thus, a very high key agreement rate can be achieved by the system. The only problem with this technique is that key generation rate is very slow. In [317], authors presented a lightweight and simple encryption technique based on PLS for BAN. The technique enables us to incorporate security with compressed sensing method during the process of sampling an analog signal.

In [318], a novel key agreement method was proposed to share PLS-based generated key without any extra hardware. In [318], encoding of channel based-information, e.g., received signal strength indicator (RSSI) data, to manic polynomial coefficients (MPC) was done by using improved Juels and Sudan (IJS) algorithm and only higher order coefficients are sent as check bits. The receiver uses the Reed-Solomon decoding algorithm to recovers sender RSSI data from the received coefficients and receiver's local RSSI data.

In [319], the authors further improved the work of [318] by proposing a new method to encode the RSSI data to MPC. The authors compared IJS encoding and Reed-solomon encoding from a different perspective and provided their advantages and disadvantages. The authors also proposed a new variation-tolerant decoding method. In [320], an optimization based PLS technique was presented. More specifically, body-worn units interact with each other in the presence of an eavesdropper under fading conditions in order to find out the most secure multi-hop path to the hub while keeping the delay constraints based on the considered application by using game-theoretic Nash bargaining concepts. The problem is modeled as the search of multi-hop topology using Nash solution in order to optimize secrecy outage probability in the uplink of a multi-hop WBAN with end-to-end delay management.

H. Vehicular and VANET Communication Systems

Similar to any wireless system, vehicular communication systems are vulnerable to many different security attacks on different layers of the OSI model [321][17]. Among these attacks is passive eavesdropping that can be performed by a malicious vehicle on the physical layer level as shown in Fig. 25. Generally speaking, the most commonly used method for achieving data confidentiality and protection against eavesdropping in vehicular systems is the classical key-based encryption approach. However, the public cryptography-based schemes rely on centralized certificate authority (CA), which is known as a weak point in VANET as it yields a single failure point. On the other hand, symmetric cryptography sustains possible attacks on key agreement and distribution processes. Moreover, the special features of VANET, where communicating vehicle nodes move with different speeds, resulting in an extremely time-varying medium, alongside the technical requirements, represented by message size, frequency, latency constraints, computational cost, communication ranges, road geometry, and the locations of the potential eavesdroppers in vehicular

[17]For obtaining more background information about VANET communication systems, we refer the reader to [400].

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2018.2878035, IEEE Communications Surveys & Tutorials

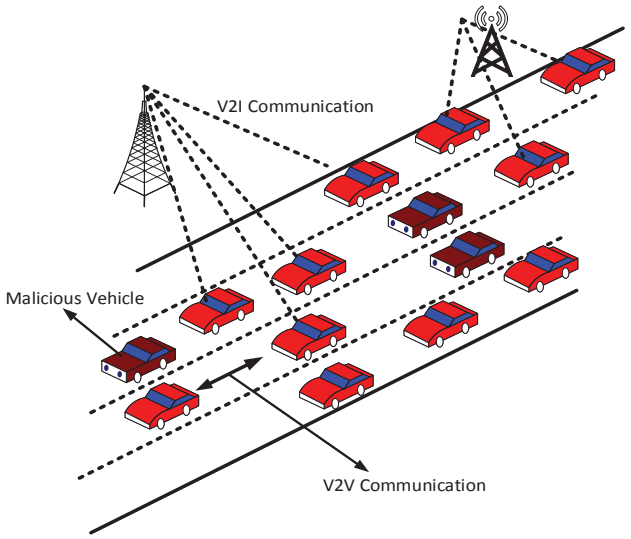

Fig. 25. Physical layer security scenario in VANET scenario.

environments; make currently used cryptographic approaches not adequate enough to be used for VANET security.

In [322], the authors aimed to solve the security issue of automotive cyber physical systems (i.e., Intra-Vehicular, V2V, V2I) by introducing a practical key generation technique that utilizes the channel reciprocity along with the spatial and temporal variations of the wireless channel. Also, the practicality of the method was validated by conducting a real-world experiment with automobiles (real communicating and self-driving cars).

In addition to channel-based key generation approach, key-less PLS approach has also been proposed to be used as an effective way for providing secrecy to vehicular systems [323]. Particularly, the road geometry and natural restriction on the potential eavesdroppers locations in vehicular environments were exploited to provide security through injecting artificial noise in a controlled direction along the lane of travel [323]. It should be stated that aside from the fact that eavesdropping is a challenging problem as the attacker cannot be detected due its passiveness and silence alongside the delay-sensitive property of VANET systems, jamming is also a very critical attack that needs real effective solution to stop it [321], [324]. In [325], the authors exploited the unique channel dynamic characteristics of a vehicular scenario to extract and generate high rate secret keys. A similar related study to the previous one was also performed in [326]. In [305], the authors used Turbo codes for secret key generation as well as compensation of channel non-reciprocity in a VANET IoT scenario.

Beside the aforementioned discussion on the application of PLS to VANET, it is worth mentioning that PLS can also be applied to other vehicular relevant networks such as vehicular social networks (VSN), which is regarded as a new emerging field of research that results from the combination of social networks with vehicular networks (VANET) [401]–[405]. It is important to mention that the confidentially issue of VSN has been tackled so far by using classical security solution such as cryptography, whereas applying the concept of PLS to VSN has been clearly studied yet. Particularly, the dynamic structure and increasing number of vehicles participating in the network results in serious threats for communication privacy. This makes the confidentiality solutions for content dissemination and data transmission in VSN challenging as cryptography alone is deemed to be insufficient. Therefore, new security alternatives such as PLS are worth to be considered for securing VSN while meeting its requirements.

I. Cognitive Radio (CR) Systems

Cognitive radio (CR)[18] has unique characteristics that allow it to solve the problem of spectrum under-utilization by accessing the spectrum of licensed (primary) users opportunistically without causing interference to their communication. CR nodes can sense and analyze their environment and then adjust the parameters based on the sensed information. The PLS in CRN is more challenging as compared to conventional wireless communication systems because of the strict need for satisfying QoS requirements of the primary network, exposure of secondary user (SU) receiver to overall interference from the primary users' (PUs) transmitters and also due to the extra susceptibility of secondary network to security threats. In the literature, a lot of physical layer security techniques have been proposed for wireless communication. Many techniques used for conventional wireless communication are applicable to CR with some modification based on above mentioned constrains and structure of CRN. The basic system model of secure CR is presented in Fig. 26.

In [327], authors investigated a scenario for PLS in which SU-transmitter sends secret information to SU-receiver using the same frequency band as primary user in the presence of a passive eavesdropper. The authors proposed a relay selection scheme that selects a trusted decode and forward relay to maximize the secrecy capacity of secondary users subjected to QoS constraints of primary users for different numbers of eavesdroppers. In [328], a multiple relay based transmission scheme for enhancing physical layer security was introduced. In order to enhance secrecy capacity, both cooperative jamming and beamforming technologies are used. The presented technique provides secure SU transmission subjected to QoS constraints of primary user receiver. In [329], a cognitive radio (CR) network was considered that consists of pair of secondary Tx and Rx with multiple secondary relays (SRs) in the presence of an eavesdropper. The Tx transmits to Rx with the help of relays in the presence of passive eavesdropper. The authors proposed relay selection algorithm for enhancing PLS.

In [330], artificial noise generation and beamforming were jointly adopted at the SU transmitter to enhance the security of MISOME primary network. In [331], authors showed that the best performance in terms of security can be achieved if perfect channel state information (CSI) is available for all links. In [332], authors investigated PLS in CRN by proposing multiuser scheduling scheme to achieve multiuser diversity in order to improve the security under QoS constraints of primary users. Specifically, a SU that maximizes the secrecy rate while

[18]For obtaining more background information about Cognitive Radio (CR) systems, we refer the reader to [406]–[408]

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2018.2878035, IEEE Communications Surveys & Tutorials

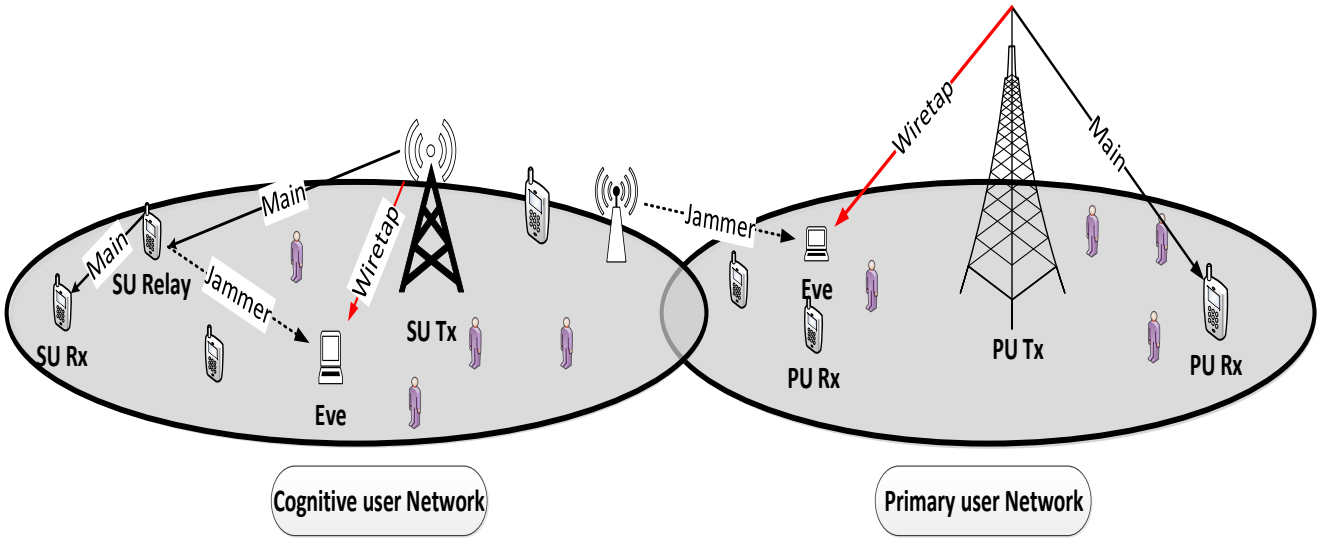

Fig. 26. Physical layer security scenario in cognitive security.

satisfying the QoS requirement of PU is scheduled to transmit its data packet. In [333], power allocation strategies over bank of idle independent parallel Gaussian wiretap channels were investigated in a cognitive radio system in the presence of a friendly jammer and an eavesdropper. In [334], the secrecy performance of a multi-antenna cognitive wiretap network was investigated. The authors considered secondary Tx communicating with the secondary Rx in the presence of an eavesdropper for both full-duplex and half-duplex cases. For the case of half-duplex, MRC is used at Bob; while for the case of full-duplex, the authors proposed selection combining/zero forcing beamforming (SC/ZFB) and SC/Selection jammer (SC/SJ) for deteriorating the performance of Eve.

In [335], the authors presented a security scheme for multiple AF relaying CCRNs against passive eavesdroppers based on collaborative beamforming. In [336], incentive-based PLS technique for PU via cooperative SU has been investigated. SU helps in the improvement of PLS for PU while getting transmission opportunities as an incentive from PU. In this work, two types of cooperation schemes have been proposed, i.e, relay-jammer scheme and cluster-beamforming scheme. In relay-jammer scheme two SUs act as a friendly jammer to secure communication of PU, while getting a fraction of access time of transmission from PU as an incentive; while in cluster beamforming schemes, the PU collaborate with a group of SUs to enhance security via collaborative beamforming against eavesdropping. Similar to [336], the authors in [338] and [337] presented a case study in which SU acts as a jammer to enhance security.

In [339], the problem of secure communication for two-hop primary system was investigated in the presence of untrusted secondary system. The secondary system is untrusted but willing to provide friendly jamming to increase security of primary network in reward of incentive in terms of getting part of slot allocated for the primary information transmission. In this work, to maximize the rate of SU under security constrained on primary user two jamming SUs were optimally selected and the time parameters in each slots were determined. In [340], two way relay secondary network was considered which can access the licensed spectrum to support its QoS requirements as long as it ensures secure communication for the primary system against malicious eavesdroppers. In order to secure primary user, the secondary system uses cooperative jamming and relaying. The power is allocated to the secondary system relaying message and jamming signal in such a way that the secrecy capacity of primary user is maximized while ensuring minimum QoS requirements of secondary system.

In [341], authors presented optimal stopping based jammer selection (OSJS) scheme for MIMO enabled CCRN. The network consists of a pair of PUs, number of Secondary User (SU) pairs, a single relay and an eavesdropper. The pair of PU needs to select a SU pair as the jamming stations. As a reward, the selected SUs are given some resources for transmission. In [342], the authors proved that if perfect knowledge of channel is available, the optimal strategy to secure MISO CRN is beamforming. The authors then extended the work to include the case of imperfect channel estimation in [343].

In [344], the authors presented optimal antenna selection (OAS) and suboptimal antenna selection (SAS) schemes for enhancing PLS of MIMO-CR system which consists of a multi-antenna SU-transmitter, SU-receiver and an eavesdropper. In OAS case, perfect knowledge of channel state information is assumed; while in SAS case, the channel state information is not available. It is shown that secrecy outage probability of SAS for MIMO-CR is better than SISO-CR while it is worse than OSA-MIMO-CR. Furthermore, it is also shown that as the number of antenna increases, the secrecy outage probability for both optimal and suboptimal case improves significantly.

In [345], secrecy outage probability analysis of OAS and

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2018.2878035, IEEE Communications Surveys & Tutorials

SAS for an underlay MIMO CRN with energy harvesting is presented for different cases related to the availability of channel state information. The CRN consists of a pair of primary nodes and secondary nodes and an eavesdropper, where the secondary transmitter is using energy harvested from primary transmitter. In [346], the authors presented a resource allocation framework for enhancing security in a two-way cooperative communication for secondary users within an OFDMA based underlay cognitive system. The target was to maximize the secrecy sum rate of secondary users. It was shown that the deployments of relays have vital role in providing non zero secrecy rate. In [409], two techniques are proposed for physical layer security of CR networks. In the first technique, authors designed secondary transceivers in order to maximize their sum rate while making sure that a threshold on the secrecy rate of PU is satisfied by using optimization algorithms. In the second technique, the authors employed the principle of interference alignment in order to eliminate the interference from SUs and PU. Thus, legitimate CR network can perform interference-free transmission while SUs disrupt the eavesdropping towards PU.

J. Radio-Frequency Identification (RFID) Systems

Due to the light processing and storage capabilities of radio frequency identification (RFID) systems including their RFID tags, using conventional cryptographic techniques becomes almost impossible and impractical in such resource constrained systems. To address this challenge, lightweight security techniques are highly required. Therefore, the authors in [347], [348] presented the first analysis on the adoption of PLS techniques in an RFID system, whose basic security model is presented in Fig. 27. In their work, the secrecy rate of RFID backscatter systems was first characterized, and then an approach for maximizing this secrecy rate by exploiting the nature and features of the RFID backscatter channel was proposed. In [349], [350], the authors investigated the PLS of MIMO-RFID system. Then, a noise-injection precoding mechanism was proposed to safeguard the system against eavesdropping with the special requirements of the backscatter RFID system taken into account. In [351], the authors proposed a novel, effective, and eavesdropping-resilient method based on randomizing the modulation and channel to secure RFID systems against an eavesdropper with multiple antennas.

K. Ultra-Wideband Communication (UWB)

Ultra-wideband communication (UWB)[19] enables broadband communication with high symbol rates for short range distances (low power transmission) by using extremely short pulse durations. This technology is standardized under the name IEEE 802.15.4 and then amended later on under the name IEEE 802.15.4a.

Besides the aforementioned advantages, the narrow time domain pulse width (in nanosecond) of UWB signals as well as their low transmission power (close to the noise level power)

[19]For obtaining more background information about Ultra-Wideband Communication (UWB), we refer the reader to [410].

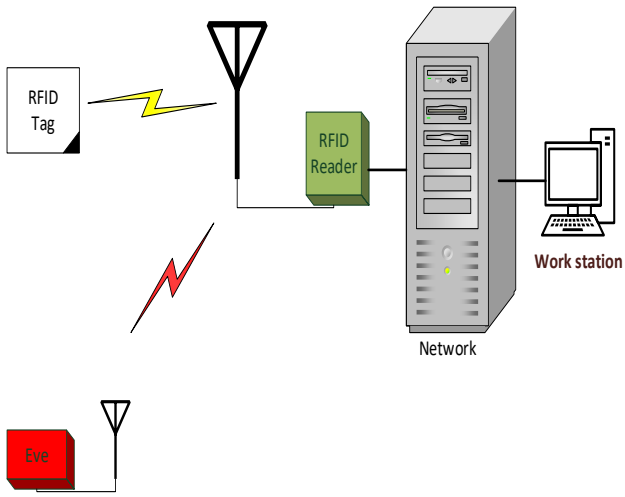

Fig. 27. Physical layer security scenario in RFID.

makes it naturally difficult for eavesdroppers to intercept and detect. Particularly, the fine and highly precise time resolution of UWB allows better channel quantization for physical layer-based secret key generation methods. This of course results in high rates of secret information that can be obtained from the shared channel characterizations between legitimate communication entities.

In [354], the authors developed secure communications in UWB based on generating secret key sequences from channel measurements instead of depending on a trusted third party to generate and distribute the keys as is the case in traditional cryptography-based systems. In particular, upper bounds on the secret key rate for UWB channels are derived and calculated, where high secure key rates are demonstrated.

In [355], the physical layer security performance of UWB systems was investigated for coherent reception and UWB transmitted-reference (TR) schemes in IEEE 802.15.4a channel models. Results for IEEE 802.15.4a channel models disclose the suitability of the UWB channel for generating sufficient secret information to be used at higher-layer protocols.

In [353], the authors presented experimental practical results related to secret key extraction from the physical properties of UWB channels. The introduced design, which is tested with real life measurements in an indoor environment, is exhibited to result in secret keys with high randomness and low mismatch percentages.

In [356], a compact hardware implementation of a digital code-shifted reference (CSR) UWB transceiver was reported, where the transmission security of the design is achieved by changing the physical properties of the transmission without the use of higher level security options. Particularly, security is achieved by altering the physical properties of the transmitted signal based on a known sequence to the communicating parties. The scheme preserves low complexity of a non-coherent reception while introducing time hopping to secure the data. The basic concept behind the adopted and implemented security scheme was presented in [355], where the time domain

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2018.2878035, IEEE Communications Surveys & Tutorials

positions of the used transmit pulses are continuously altered (i.e., time hopping) to secure the transmitted data. In this case, Eve has to find the exact location of that small pulse that exists in a time frame composed of hundreds of possible candidate pulse locations. In [357], the secrecy performance of transmit antenna selection in UWB was analyzed and investigated in a MISO scenario.

L. Device to Device (D2D) Communication

As is the case with any new promising technology, D2D communication[20] has its own unique structure and topology that is specifically designed to benefit and support the needs of future wireless networks. Particularly, the advantages of this technology is realized by reusing the spectrum resources for communication between the devices located in a close proximity to each other in a peer-to-peer manner and without the need to the network infrastructure. This technology, which has recently been adopted in LTE-advance release 12, not only provides better data rates (throughput) and reduced power wastage by utilizing the system resources judiciously but also yields flexibility in interference management between D2D users and traditional cellular users.

Interestingly, due to the additional interference that D2D topology creates, one can predict that PLS can be improved when D2D communication is employed. Motivated by this intuitive observation, In [358], Yue *et al.* introduced and applied for the first time in the literature the PLS concept to D2D communication scenario, where it is shown that the interference caused by D2D topology can be helpful to cellular users in defending against eavesdropping problem. The goal was to enable each D2D pair achieve its own transmission satisfactorily while meeting the secrecy requirements of normal cellular users. To attain this goal, optimal power allocation mechanism along with an access control procedure was proposed.

The authors of [359] re-emphasized the advantage of D2D paradigm in improving the secrecy performance, where the secrecy outage probability for the D2D and cellular systems was derived, and compared in a multi-antenna eavesdropper scenario. In [360], Shen *et al.* introduced a secure and efficient key agreement protocol for D2D paradigm and then implemented it using Android smart-phones.

To optimize the system secrecy rate, Zhang *et al.* [361] derived and obtained the optimal joint power control of both the cellular and D2D pairs' links. To enhance the secrecy further, the authors proposed a joint power and access control scheme with optimal selection process of D2D pair. In [363], Qu *et al.* also studied the optimal power allocation between D2D pairs being eavesdropped by cellular users. In [362], the authors explored the cooperation issue between nodes by spectrum sharing when PLS concept is applied and employed into the D2D communication scenario within the cellular network. In [364], artificial noise was employed in a D2D scenario to improve secrecy.

[20]For obtaining more background information about Device-to-Device (D2D) communication, we refer the reader to [411], [412].

Later on, many more studies about PLS for D2D communication in various scenario were conducted and performed in the literature [365]–[380]. One inference to mention here is that PLS for D2D has become a new emerging multi-goal research area by itself, where secrecy and interference are the key factors driving the research in this direction.

M. Unmanned Aerial Vehicle (UAV) Communication

Due to the rapid growth in the number of semi-autonomous and autonomous vehicles, for example, Unmanned Aerial Vehicles (UAVs)[21], UAV-enabled mobile relaying has recently received too much attention. The basic model for UAVs based communication with respect to PLS is presented in Fig. 29. In [381], authors maximized the secrecy rate of four nodes system setup that includes a source, an unmanned aerial vehicles (UAVs)-enabled mobile relay, destination and an eavesdrop. The authors developed an iterative algorithm by exploiting the difference of concave program to solve the non-convex optimization problem.

In [382], authors proposed a tractable analysis framework in order to evaluate the security, secrecy energy efficiency (SEE) performance and reliability of a UAV-enabled communication system that consists of multiple UAV-enabled legitimate transmitters, receivers and eavesdroppers. This is performed by considering multi-antenna techniques and threshold-based access schemes. In the first step, the activation probability of UAV-enabled transmitters and association probability of randomly located receivers are exploited. Then, reliability, SEE and security of the UAV-enabled networks are analyzed.

In [383], the authors maximized the secrecy rate of system by joint optimization of transmit power and UAV's trajectory over a finite horizon by considering mobile UAVs. The proposed non-convex problem was solved by an iterative algorithm that is based on successive convex optimization and block coordinate descent methods.

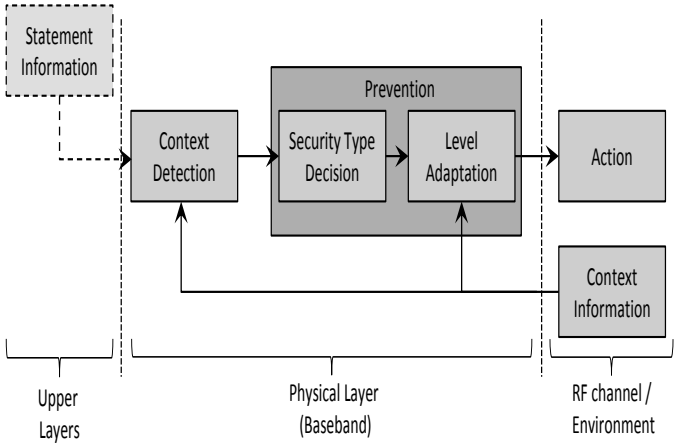

Fig. 28. System model for cognitive security (environment, scenario and context adaptive security).

[21]For obtaining more background information about Unmanned Aerial Vehicles (UAVs), we refer the reader to [413], [414].

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2018.2878035, IEEE Communications Surveys & Tutorials

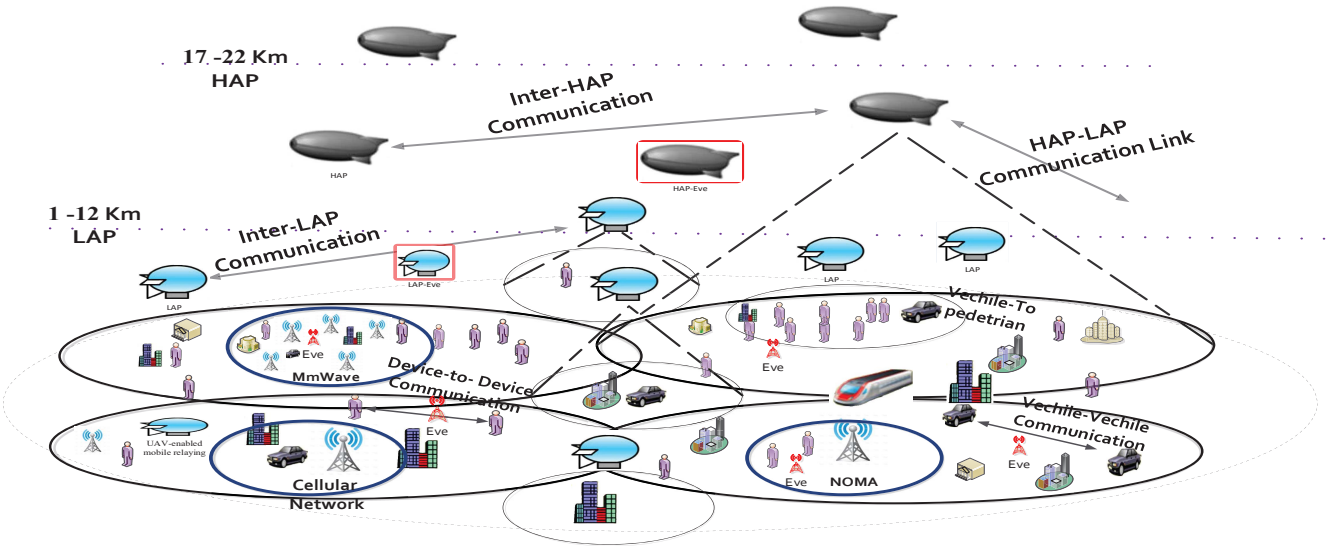

Fig. 29. Physical layer security concepts for future aerial and terrestrial multi-Hetnets.

VI. Challenges, Recommendations and Future Research Directions

A. Minimizing Drawbacks of Security Approaches while Maximizing their Merits

Based on the aforementioned material we have presented and specifically the block diagrams (Fig.3 and Fig.4) that concisely summarize the advantages and disadvantages of the existing physical layer security techniques and their branches, one can simply conclude that each security track and approach has its own Pros. (merits) and Cons (demerits). In particular, what may be suitable for some applications, systems, scenarios, and channel conditions might not be good for others. Thus, based on these substantial inferences and results, which have been made possible due to the security framework we carefully structured and offered, we can favor one method over another according to the our needs and requirements. Since each direction and each method has some promising security advantages in one side and some flaws as well in the other side. Therefore, it is worth devoting some of our research efforts on developing new advanced security methods that are capable of minimizing the drawbacks/side effects of these security tracks while maximizing their merits. This goal can be attained through designing practical techniques which can help not only in security, but also in satisfying the other communication system requirements such as reliability, complexity, power efficiency, spectral efficiency, delay and complexity. It is firmly anticipated that any technique adopts this approach will certainly make it interesting and valuable for both research and industry communities.

B. Cross Layer Security

Another futuristic and promising research area, which is not yet investigated heavily in the literature, is cross layer security design such as cross MAC/PHY layer security, cross NET/PHY layer security, cross NET/MAC/PHY layer security, etc. These new security approaches aim at involving the upper-layers such as MAC and network layers in the physical security design process. This target can be achieved through exploiting the functionalities and mechanisms of these layers for security purposes. For example, the degree of freedom existing in ARQ as a MAC layer mechanism along with maximal ratio combination, adaptive modulation, artificial noise, and other techniques as physical layer mechanisms can be adopted for security.

C. Adaptation is Good for Enhancing Security as well as Other System Performances

Adaptation processes are expected to dominate the design principle of future wireless networks because adaptive designs not only enhance the efficiency and performance of legitimate receivers, but also increase the security level of our systems. Adaptation processes can include channel-based adaptive precoding, partial pre-equalization, optimized waveforms, adjustable filtering, resource allocation, parameter optimization and joint structural design of transmitters and receivers based on the channel between them (i.e., channel-based pre-processing and post-processing). This transmission mechanism is very effective and particularly useful for the cases when the transmitter is able to know some pre-information about the statistics of the malicious eavesdroppers and the specific spatial regions that we want our communication to be secure in.

In spite of the many advantages that adaptation-based techniques offer, they are unfortunately not sufficient enough in scenarios where many eavesdroppers can collaborate and multiple different observations of the transmitted signal can be acquired from many spatial locations by Eve. Thus, a promising direction can be the integration of adaptation-based approaches with other security techniques (e.g., artificial noise) in order to maintain an adequate secrecy level against multiple eavesdroppers' cooperation and colluding while keeping the inherent merits of the adaptation-based approaches.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/COMST.2018.2878035, IEEE Communications Surveys & Tutorials

D. Cognitive Security

Cognitive security is another promising new research direction: In [415], authors proposed a novel concept of cognitive security (CS) for wireless communication that can provide adaptive, reliable, robust and comprehensive security solutions for wireless communication. In CS, physical layer security concept is exploited in a unique way, such that the radio first detects and combines the information from environmental conditions and radio channel. Afterwards, based on detected information, it detects the respective context. After detecting the context, radio adapts different propagation characteristics and takes necessary precautions to provide security. The basic concept for cognitive security (CS) is presented in Fig. 28.

E. Channel Reciprocity Calibration and Robust Channel Estimation are Key for Having Successful Security Schemes

Since most of the physical security techniques are completely based on exploiting the characteristics of the channel and its availability at both the transmitter and receiver sides, robust channel estimation along with reciprocity calibration becomes inevitable challenging task to encounter as it is difficult to achieve in practice. Thus, the effect of imperfect channel estimation and reciprocity mismatch should be taken into account when a new security method is designed to make sure that it is robust against these drawbacks; and in case it is not, then efficient practical channel calibration solutions are needed to tackle these issues. Additionally, although most of the aforementioned security directions consider somewhat the practical assumption of the fact that Bob's channel is independent of Eve in a wireless environment, which can be satisfied when they are separated apart by at least half a wavelength; this is still not always true, where there are cases and specific poor scattering environments where there might be a strong correlation between Bob and Eve [416]. In this case, the level of physical layer security will reduce significantly (e.g., secrecy will be exactly zero if both Bob and Eve are placed extremely close to each other). Thus, re-examining and investigating the existing physical layer security techniques under these conditions may give new insights about the practicality and robustness levels of the current available security methods.

F. Channel-based Key Generation is challenging in Poor Scattering Environments

For channel-based secret key generation approach, extracting keys with high rates remains a very challenging task, especially for poor scattering or line of site (LOS) environments, where there is no much randomness or variations in the channel due to having long coherence time. To address this challenge, a few recent studies in the literature [417]–[422] have proposed creating virtual random channel [417] (by using opportunistic randomized beamforming [423] along with diversity) or by producing artificial interference [418] that can be used to generate high secret key rates with good entropy independent of the actual mobility and variations of the channel. Due to the practicality and super benefits provided by this channel-independent secret key generation approach [138], it is foreseen that more research studies and works related to deep performance analysis, investigation and practical implementation are needed in order to verify and validate the applicability of this approach for integration and extensions to other wireless systems and scenarios.

G. Pre-coding and Artificial Noise-based Security Techniques Cause Peak-to-Average Power Ratio (PAPR) Increase

The effect of the pre-coding and artificial noise-based security techniques on the peak-to-average power ratio (PAPR), which is associated with power amplifier non-linearity problem, is mostly forgotten in the literature of physical layer security. Particularly, there are very little works about this practical important issue, which is so critical to a level that it may impede and even prohibit the applicability of many of the artificial noise-based security techniques in realistic situations. Thus, such serious practical issues should be examined for all the previously provided physical layer security techniques via revisiting them from a different perspective in order to test and investigate whether these security techniques cause PAPR increase or not; and if they do, then efficient signal processing techniques need to be designed in order to provide proper solutions to this problem. In the meanwhile, researchers, who are developing new security algorithms are strongly recommended to take such an issue into account while designing their security schemes. In [424], the researchers showed that the famous artificial noise based technique proposed by Nagi and Goel in [127] creates high PAPR similar to that produced by an OFDM signal due to the accidental in-phase addition (superposition) of AN subspaces and the data subspaces. To mitigate the PAPR of the transmitted signal, an angle rotation based technique was proposed to reduce the PAPR, while maintaining the same secrecy capacity performance as that of the original artificial noise aided method. In [123], we proposed to either change the distribution of the added AN from Gassuain to uniform in flat fading environments or to use an optimized AN that not only avoids PAPR increase but also helps reduce the PAPR of OFDM signal transmission over frequency selective channels (i.e., time dispersive channel).

H. Line of Site (LOS) Environment is a Challenging Scenario for Security

There are some extremely challenging security scenarios such as those related to line of site (LOS) environments and the eavesdropper is located within the same direction of the legitimate user. In this case, many of the physical layer security techniques such as conventional linear beamforming [25], [275], [425], classical antenna subset modulation [105], directional modulation [426], artificial noise-based MIMO techniques [127], etc. will fail to provide security. Generally speaking, there is a huge need to design much more practical PLS techniques that can sustain its applicability in scenarios of poor scattering (non-fading), static time invariant (non-dynamic), or non-dispersive channels (no multipath), where most of the existing security techniques that exploit the opposite of these scenarios may not be able to provide physical security.

I. The Joint Design of Secrecy, Reliability, Throughput, and Delay is Needed to Achieve a Good Trade-off

The joint optimal design of secrecy, reliability, throughput, delay and the trade-off among them is another important area, which is not yet well investigated in the literature. In general, providing physical secrecy constraints usually come at the expense of compromising other system requirements. For example, channel coding-based techniques sacrifice spectral efficiency, while artificial noise-based techniques compromise power efficiency, where unnecessary power is transmitted in this case. Thus, an optimal design that takes the quality of service requirements such as delay, throughput, and packet error rate into account while insuring security, is an essential track in future research security work, for example, Fig. 29 presents the future communication model with respect to PLS. Recent work has shown that the previous knowledge of the type of running application (service) at user side is a very advantageous feedback that should be taken into account during the phase of security design process to ensure conveying a certain service confidentially. The reason for this is that, when we get to know the application run by the legitimate user, we adopt our transmission parameters exactly according to user needs, no more no less, while these parameters ensure in the same time that Eve is operating below these requirements making it difficult for her to get the required QoS. Interestingly, this kind of security design approaches states that strong secrecy is not always needed to provide a perfect secure service.

J. The Requirements of Different Type of Services Need to be Included in the Secrecy Design Equation

Most of the PLS techniques and approaches whether they are key-based (Shannon's model) or key-less (Wyner's model) are basically designed to merely secure messaging service without considering the actual required security level of other types of used services such as voice, video, VOIP, streaming, gaming, URLLC, mMTC, etc. For this kind of services, the ultimate goal is to deliver them to the users reliably and within the determined and standardized Quality of Service (QoS) requirements. In such a situation, it is anticipated that perfect secrecy (i.e., perfectly zero information leakage to Eve) is not always needed to provide a perfectly secure service. In reality, each service has different QoS requirements than the others, and if we ensure that Eve is operating below these requirements, then practical service-based secrecy can be guaranteed. Thus, a promising research direction would be to redesign the existing PLS techniques from a much more practical perspective where the actual QoS requirements of real services such as URLLC, mMTC, VOIP, video, etc. are taken into account.

K. Hybrid Security Techniques

Last but not least, designing hybrid security techniques which can provide more than one level of security, i.e., two levels (sources) of security: one is coming from an SINR-based technique, while the other is coming either from a complexity-based technique or from conventional cryptographic based techniques. This will help to make the security scheme more robust and immune against eavesdropping.

VII. Conclusion

In this paper, we have proposed a new unique framework for classifying the existing physical layer security methods against wireless passive eavesdropping considering practical assumptions. The main purpose is to make it simple, understandable and tractable so that researchers, engineers and students can get better understanding of the big picture of physical layer security. Specifically, security techniques have been divided into two primary approaches: SINR-based approach and complexity-based approach. The first approach was classified into three major categories: first, secrecy channel codes; second, security techniques based on adaptation with respect to the legitimate users channel; third, schemes based on adding intentional interfering signals on top of the transmitted information signals. The second approach, which is associated with the mechanisms of extracting secret sequences from the shared channel, was classified into two main categories based on which layer the secret sequence obtained by channel quantization is applied on. The implementation of each one of these categories was divided and classified into three main signal domains: time, frequency and space. For each one of these domain, several examples were given and illustrated along with reviewing the most recent security advances in each domain. Moreover, the lessons learned, advantages, and disadvantages of each technique have been discussed to give an insight on the trade-off process between security and the other communication requirements such as reliability, capacity, power efficiency and complexity. The recent applications of PLS techniques into emerging areas like VLC, BAN, PLC, IoT, smart grid, mm-Wave, cognitive radio, vehicular, UAV, UWB, D2D, RFID, index modulation and 5G systems including secure waveforms and multiple accessing, are also reviewed and discussed. The paper has been concluded with some recommendations and future directions for designing robust, power efficient and strong security methods for current and future wireless systems.

References

[1] C. E. Shannon, "Communication Theory of Secrecy Systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, oct 1949.
[2] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, oct 1975.
[3] Y.-S. Shiu, S. Chang, H.-C. Wu, S. Huang, and H.-H. Chen, "Physical layer security in wireless networks: a tutorial," *IEEE Wireless Commun.*, vol. 18, no. 2, pp. 66–74, apr 2011.
[4] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surv. Tuts.*, vol. 16, no. 3, pp. 1550–1573, jan 2014.
[5] Y. Liu, H. H. Chen, and L. Wang, "Physical layer security for next generation wireless networks: Theories, technologies, and challenges," *IEEE Commun. Surv. Tutorials*, vol. 19, no. 1, pp. 347–376, First quarter 2017.
[6] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proc. of the IEEE*, vol. 104, no. 9, pp. 1727–1765, Sept 2016.
[7] H. V. Poor and R. F. Schaefer, "Wireless physical layer security," *Proc. of the National Academy of Sciences*, vol. 114, no. 1, pp. 19–26, 2017.

[8] M. Bloch and J. Barros, *Physical-layer security: From information theory to security engineering*. Cambridge University Press, Aug. 2008.

[9] R. Liu and W. Trappe, *Securing wireless communications at the physical layer*. Springer, 2010.

[10] X. Zhou, L. Song, and Y. Zhang, *Physical layer security in wireless communications*. CRC Press Taylor and Francis Group, 2013.

[11] Y.-W. P. Hong, P.-C. Lan, and C.-C. J. Kuo, *Signal processing approaches to secure physical layer communications in multi-antenna wireless systems*. New York, NY, USA: Springer, 2014.

[12] M. Baldi and S. Tomasin, *Physical and data-link security techniques for future communication systems*, ser. 1876-1100. Springer International Publishing, 2016.

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

[14] R. Bassily, E. Ekrem, X. He, E. Tekin, J. Xie, M. R. Bloch, S. Ulukus, and A. Yener, "Cooperative security at the physical layer: A summary of recent advances," *IEEE Sig. Process. Mag.*, vol. 30, no. 5, pp. 16–28, Sep 2013.

[15] M. Bloch, M. Hayashi, and A. Thangaraj, "Error-control coding for physical-layer secrecy," *Proc. IEEE*, vol. 103, no. 10, pp. 1725–1746, Oct 2015.

[16] R. K. Sharma and D. B. Rawat, "Advances on security threats and countermeasures for cognitive radio networks: A survey," *IEEE Commun. Surv. Tuts.*, vol. 17, no. 2, pp. 1023–1043, 2015.

[17] C. Shahriar, M. La Pan, M. Lichtman, T. C. Clancy, R. McGwier, R. Tandon, S. Sodagari, and J. H. Reed, "Phy-layer resiliency in OFDM communications: A tutorial," *IEEE Commun. Surv. Tuts.*, vol. 17, no. 1, pp. 292–314, 2015.

[18] X. Chen, C. Zhong, C. Yuen, and H.-H. Chen, "Multi-antenna relay aided wireless physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 12, pp. 40–46, Dec 2015.

[19] E. Jorswieck, S. Tomasin, and A. Sezgin, "Broadcasting into the uncertainty: Authentication and confidentiality by physical-layer processing," *Proc. IEEE*, vol. 103, no. 10, pp. 1702–1724, Oct 2015.

[20] X. Chen, D. W. K. Ng, W. H. Gerstacker, and H. H. Chen, "A survey on multiple-antenna techniques for physical layer security," *IEEE Commun. Surv. Tuts.*, vol. 19, no. 2, pp. 1027–1053, Secondquarter 2017.

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

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

[23] Z. E. Ankarali, Q. H. Abbasi, A. F. Demir, E. Serpedin, K. Qaraqe, and H. Arslan, "A comparative review on the wireless implantable medical devices privacy and security," in *2014 4th Int. Conf. on Wireless Mob. Commun. and Healthcare - Transforming Healthcare Through Innovations in Mobile and Wireless Technologies (MOBIHEALTH)*, Nov 2014, pp. 246–249.

[24] M. H. Yilmaz and H. Arslan, "A survey: Spoofing attacks in physical layer security," in *2015 IEEE 40th Local Comput. Networks Conf. Work. (LCN Work.)*, oct 2015, pp. 812–817.

[25] W. C. Liao, T. H. Chang, W. K. Ma, and C. Y. Chi, "QoS-based transmit beamforming in the presence of eavesdroppers: An optimized artificial-aoise-aided approach," *IEEE Trans. Signal Process.*, vol. 59, no. 3, pp. 1202–1216, 2011.

[26] M. Li, S. Kundu, D. A. Pados, and S. N. Batalama, "Waveform design for secure SISO transmissions and multicasting," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1864–1874, sep 2013.

[27] H. Reboredo, J. Xavier, and M. R. D. Rodrigues, "Filter design with secrecy constraints: The MIMO gaussian wiretap channel," *IEEE Trans. Signal Process.*, vol. 61, no. 15, pp. 3799–3814, 2013.

[28] A. Subramanian, A. T. Suresh, S. Raj, A. Thangaraj, M. Bloch, and S. McLaughlin, "Strong and weak secrecy in wiretap channels," in *2010 6th Int. Symp. on Turbo Codes Iterative Inf. Process.* IEEE, Sep 2010, pp. 30–34.

[29] E. Guvenkaya, J. M. Hamamreh, and H. Arslan, "On physical-layer concepts and metrics in secure signal transmission," *Phy. Commun.*, vol. 25, pp. 14 – 25, Aug. 2017.

[30] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun 2008.

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

[32] J. M. Hamamreh, M. Yusuf, T. Baykas, and H. Arslan, "Cross MAC/PHY layer security design using ARQ with MRC and adaptive modulation," in *IEEE Wireless Commun. and Netw. Conf., WCNC 2016, Doha, Qatar, April 3-6, 2016*, 2016, pp. 1–7.

[33] K. Morrison and D. Goeckel, "Secrecy rate pair constraints for secure throughput," in *IEEE Mil. Commun. Conf. (MILCOM)*, oct 2014, pp. 479–484.

[34] B. He, X. Zhou, and A. L. Swindlehurst, "On secrecy metrics for physical layer security over quasi-static fading channels," *IEEE Trans. Wireless Commun.*, vol. 15, no. 10, pp. 6913–6924, Oct 2016.

[35] S. Leung-Yan-Cheong and M. Hellman, "The gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, Jul 1978.

[36] M. R. Bloch and J. N. Laneman, "Strong secrecy from channel resolvability," *IEEE Trans. Inf. Theory*, vol. 59, no. 12, pp. 8077–8098, Dec 2013.

[37] L. H. Ozarow and A. D. Wyner, "Wire-tap channel II," *Bell Syst. Tech.*, vol. 63, pp. 2135–2157, 1984.

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

[39] R. Liu, Y. Liang, H. V. Poor, and P. Spasojevic, "Secure nested codes for type ii wiretap channels," in *2007 IEEE Inf. Theory Work.* IEEE, sep 2007, pp. 337–342.

[40] C.-H. Hsu and A. Anastasopoulos, "Capacity achieving LDPC codes through puncturing," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4698–4706, oct 2008.

[41] D. Klinc, S. W. McLaughlin, and J. Barros, "LDPC codes for the gaussian wiretap channel," *IEEE Trans. Inf. Forensics Secur.*, vol. 6, no. 3, pp. 532–540, Sep. 2011.

[42] N. Maturo, M. Baldi, M. Bianchi, and F. Chiaraluce, "Security gap performance of some LDPC code constructions," in *2013 36th Int. Conf. Telecommun. Sig. Process.*, jul 2013, pp. 77–81.

[43] A. Nooraiepour and T. M. Duman, "Randomized serially concatenated ldgm codes for the gaussian wiretap channel," *IEEE Commun. Lett.*, vol. 22, no. 4, pp. 680–683, April 2018.

[44] M. Baldi, G. Ricciutelli, N. Maturo, and F. Chiaraluce, "Performance assessment and design of finite length LDPC codes for the Gaussian wiretap channel," in *2015 IEEE Int. Conf. on Commun. Wkshp. (ICCW)*, June 2015, pp. 435–440.

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

[46] O. O. Koyluoglu and H. El Gamal, "Polar coding for secure transmission and key agreement," *IEEE Trans. Inf. Forensics Secur.*, vol. 7, no. 5, pp. 1472–1483, Oct 2012.

[47] E. Sasoglu and A. Vardy, "A new polar coding scheme for strong security on wiretap channels," in *2013 IEEE Int. Symp. Inf. Theory*, Jul 2013, pp. 1117–1121.

[48] Y. Zhang, A. Liu, C. Gong, G. Yang, and S. Yang, "Polar-LDPC concatenated coding for the AWGN wiretap channel," *IEEE Commun. Lett.*, vol. 18, no. 10, pp. 1683–1686, oct 2014.

[49] L. Song, L. Xie, H. Chen, and K. Wang, "A feedback-based secrecy coding scheme using polar code over wiretap channels," in *2014 Sixth Int. Conf. Wirel. Commun. Sig. Process.*, Oct 2014, pp. 1–6.

[50] R. A. Chou, M. R. Bloch, and E. Abbe, "Polar coding for secret-key generation," *IEEE Trans. Inf. Theory*, vol. 61, no. 11, pp. 6213–6237, Nov 2015.

[51] R. A. Chou and M. R. Bloch, "Polar coding for the broadcast channel with confidential messages," in *2015 IEEE Inf. Theory Work.*, Apr 2015, pp. 1–5.

[52] Y. P. Wei and S. Ulukus, "Polar coding for the general wiretap channel with extensions to multiuser scenarios," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 2, pp. 278–291, Feb 2016.

[53] T. C. Gulcu and A. Barg, "Achieving secrecy capacity of the wiretap channel and broadcast channel with a confidential component," in *2015 IEEE Inf. Theory Wkshp. (ITW)*, April 2015, pp. 1–5.

[54] Y. Zhang, Z. Yang, A. Liu, and Y. Zou, "Secure transmission over the wiretap channel using polar codes and artificial noise," *IET Commun.*, vol. 11, no. 3, pp. 377–384, 2017.

[55] C. Ling, L. Luzzi, J. C. Belfiore, and D. Stehl, "Semantically secure lattice codes for the gaussian wiretap channel," *IEEE Trans. Inf. Theory*, vol. 60, no. 10, pp. 6399–6416, Oct 2014.

[56] L. Liu, Y. Yan, and C. Ling, "Achieving secrecy capacity of the Gaussian wiretap channel with polar lattices," *IEEE Trans. Info. Theory*, vol. 64, no. 3, pp. 1647–1665, March 2018.

[57] F. Oggier, P. Sol, and J. C. Belfiore, "Lattice codes for the wiretap gaussian channel: Construction and analysis," *IEEE Trans. Info. Theory*, vol. 62, no. 10, pp. 5690–5708, Oct 2016.

[58] A. Nooraiepour and T. M. Duman, "Randomized convolutional codes for the wiretap channel," *IEEE Trans. Commun.*, vol. 65, no. 8, pp. 3442–3452, Aug 2017.

[59] C. Cao, H. Li, Z. Hu, W. Liu, and X. Zhang, "Physical-layer secrecy performance in finite blocklength case," in *2015 IEEE Glob. Commun. Conf. (GLOBECOM)*, Dec 2015, pp. 1–6.

[60] W. Yang, R. F. Schaefer, and H. V. Poor, "Finite-blocklength bounds for wiretap channels," in *2016 IEEE Inter. Symp. Info. Theory (ISIT)*, July 2016, pp. 3087–3091.

[61] I. M. Kim, B. H. Kim, and J. K. Ahn, "BER-based physical layer security with finite codelength: Combining strong converse and error amplification," *IEEE Trans. Commun.*, vol. 64, no. 9, pp. 3844–3857, Sept 2016.

[62] M. Baldi, G. Ricciutelli, N. Maturo, and F. Chiaraluce, "Performance assessment and design of finite length LDPC codes for the gaussian wiretap channel," in *2015 IEEE Inter. Conf. Commun. Workshop (ICCW)*, June 2015, pp. 435–440.

[63] Y. Polyanskiy, H. V. Poor, and S. Verdu, "Channel coding rate in the finite blocklength regime," *IEEE Trans. Info. Theory*, vol. 56, no. 5, pp. 2307–2359, May 2010.

[64] Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2470–2492, June 2008.

[65] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct 2008.

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

[67] M. Taki and M. Sadeghi, "Spectral efficiency optimized secure broadcasting using adaptive modulation, coding and transmit power," in *2013 1st Int. Conf. Commun. Sig. Process. Appl.* IEEE, Feb 2013, pp. 1–5.

[68] S. Tomasin and N. Laurenti, "Secure HARQ with multiple encoding over block fading channels: channel set characterization and outage analysis," *IEEE Trans. Inf. Forensics Secur.*, vol. 9, no. 10, pp. 1708–1719, Oct 2014.

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

[70] Z. Zhong, L. Jin, K. Huang, and M. Yi, "A channel matched design of LDPC based secrecy coding for the fast fading channel," in *2014 8th Int. Conf. Sig. Process. Commun. Syst.*, Dec 2014, pp. 1–5.

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

[72] H. M. Furqan, J. M. Hamamreh, , and H. Arslan, "Enhancing physical layer security of OFDM systems using channel shortening," in *IEEE Annual Int. Symp. on Personal, Indoor, and Mobile Radio Commun., PIMRC 2017, Montreal, Canada, Oct., 8-13*, 2017, pp. 100–105.

[73] A. Khisti, A. Tchamkerten, and G. W. Wornell, "Secure broadcasting over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2453–2469, Jun 2008.

[74] Z. Rezki, A. Khisti, and M.-S. Alouini, "On the secrecy capacity of the wiretap channel with imperfect main channel estimation," *IEEE Trans. Commun.*, vol. 62, no. 10, pp. 3652–3664, Oct 2014.

[75] H. Jeon, N. Kim, J. Choi, H. Lee, and J. Ha, "Bounds on secrecy capacity over correlated ergodic fading channels at high SNR," *IEEE Trans. Inf. Theory*, vol. 57, no. 4, pp. 1975–1983, Apr 2011.

[76] X. Sun, J. Wang, W. Xu, and C. Zhao, "Performance of secure communications over correlated fading channels," *IEEE Signal Process. Lett.*, vol. 19, no. 8, pp. 479–482, Aug 2012.

[77] O. Gungor, J. Tan, C. E. Koksal, H. El-Gamal, and N. B. Shroff, "Secrecy outage capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 59, no. 9, pp. 5379–5397, Sep 2013.

[78] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, "On the throughput of secure Hybrid-ARQ protocols for Gaussian block-fading channels," *IEEE Trans. Inf. Theory*, vol. 55, no. 4, pp. 1575–1591, Apr 2009.

[79] E. Guvenkaya and H. Arslan, "Secure communication in frequency selective channels with fade-avoiding subchannel usage," in *2014 IEEE Int. Conf. Commun. Work. ICC 2014*. IEEE, jun 2014, pp. 813–818.

[80] X. Chen, H. Qin, L. Xiao, M. Zhao, and J. Wang, "Power-efficient joint resource allocation for multiuser wiretap OFDM channels," in *Commun. Work. (ICCW), 2015 IEEE Int. Conf.* IEEE, jun 2015, pp. 2862–2867.

[81] M. Yusuf and H. Arslan, "Enhancing physical-layer security in wireless communications using signal space diversity," in *MILCOM - 2016 IEEE Milit. Commun. Conf.*, Nov 2016, pp. 1190–1194.

[82] ——, "Controlled Inter-carrier Interference for Physical Layer Security in OFDM Systems," in *IEEE Veh. Technol. Conf. (VTC-Fall)*, Sept. 2016.

[83] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Secure pre-coding and post-coding for OFDM systems along with hardware implementation," in *13th Int. Wireless Commun. and Mobile Comput. Conf., IWCMC 2017, Valencia, Spain, Jun., 26-30, 2017*, 2017, pp. 1338–1343.

[84] J. M. Hamamreh, E. Basar, and H. Arslan, "OFDM-subcarrier index selection for enhancing security and reliability of 5G URLLC services," *IEEE Access*, vol. 5, pp. 25 863–25 875, 2017.

[85] M. Baldi, M. Bianchi, and F. Chiaraluce, "Coding with scrambling, concatenation, and HARQ for the AWGN wire-tap channel: A security gap analysis," *IEEE Trans. Inf. Forensics Secur.*, vol. 7, no. 3, pp. 883–894, Jun 2012.

[86] M. Le Treust, L. Szczecinski, and F. Labeau, "Secrecy and rate adaptation for secure HARQ protocols," in *2013 IEEE Inf. Theory Work.* IEEE, Sep 2013, pp. 1–5.

[87] Z. Mheich, M. L. Treust, F. Alberge, P. Duhamel, and L. Szczecinski, "Rate adaptive secure HARQ protocol for block-fading channels," in *2014 22nd European Sig. Process. Conf. (EUSIPCO)*, Sept 2014, pp. 830–834.

[88] Z. Mheich, M. L. Treust, F. Alberge, and P. Duhamel, "Rate adaptation for incremental redundancy secure HARQ," *IEEE Trans. Commun.*, vol. 64, no. 2, pp. 765–777, Feb 2016.

[89] S. Yan, N. Yang, G. Geraci, R. Malaney, and J. Yuan, "Optimization of code rates in SISOME wiretap channels," *IEEE Trans. Wirel. Commun.*, vol. 14, no. 11, pp. 6377–6388, Nov 2015.

[90] Q. Du, L. Sun, P. Ren, and Y. Wang, "Statistical security model and power adaptation over wireless fading channels," in *2015 Int. Conf. Wirel. Commun. Signal Process.* IEEE, Oct 2015, pp. 1–6.

[91] J. M. Hamamreh and H. Arslan, "Time-frequency characteristics and papr reduction of otdm waveform for 5G and beyond," in *2017 10th Inter. Conf. Elect. Electr. Eng. (ELECO)*, Nov 2017, pp. 681–685.

[92] F. Renna, N. Laurenti, and H. V. Poor, "Physical-layer secrecy for OFDM transmissions over fading channels," *IEEE Trans. Inf. Forensics Secur.*, vol. 7, no. 4, pp. 1354–1367, 2012.

[93] N. Laurenti, S. Tomasin, and F. Renna, "Resource allocation for secret transmissions on parallel rayleigh channels," in *2014 IEEE Int. Conf. Commun. ICC 2014*, 2014, pp. 2209–2214.

[94] S. Karachontzitis and S. Timotheou, "Security-aware max-min resource allocation in multiuser OFDMA downlink," *IEEE Trans. Inf. Forensics Secur.*, vol. 10, no. 3, pp. 529–542, 2015.

[95] C. Cai, Y. Cai, R. Wang, W. Yang, and W. Yang, "Resource allocation for physical layer security in cooperative OFDM networks," in *2015 Int. Conf. Wirel. Commun. Sig. Process.* IEEE, Oct 2015, pp. 1–5.

[96] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas I: The MISOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088–3104, 2010.

[97] ——, "Secure transmission with multiple antennas-part II: The mimome wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515–5532, 2010.

[98] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Info. Theory*, vol. 57, no. 8, pp. 4961–4972, Aug 2011.

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

[100] Z. Li, W. Trappe, and R. Yates, "Secret communication via multi-antenna transmission," in *Inf. Sci. Syst. 2007. CISS '07. 41st Annu. Conf.*, 2007, pp. 905–910.

[101] S. Shafiee and S. Ulukus, "Achievable Rates in Gaussian MISO Channels with Secrecy Constraints," in *Inf. Theory, 2007. ISIT 2007. IEEE Int. Symp.*, 2007, pp. 2466–2470.

[102] M. P. Daly and J. T. Bernhard, "Directional modulation technique for phased arrays," *IEEE Trans. Antennas Propag.*, vol. 57, no. 9, pp. 2633–2640, 2009.

[103] Z. Rezki and M. S. Alouini, "On the finite-SNR diversity-multiplexing tradeoff of zero-forcing transmit scheme under secrecy constraint," in *IEEE Int. Conf. on Commun. Wkshps (ICC Wkshps)*, June 2011, pp. 1–5.

[104] A. Mukherjee and A. L. Swindlehurst, "Robust beamforming for security in MIMO wiretap channels with imperfect CSI," *IEEE Trans. Signal Process.*, vol. 59, no. 1, pp. 351–361, 2011.

[105] N. Valliappan, A. Lozano, and R. W. Heath, "Antenna subset modulation for secure millimeter-wave wireless communication," *IEEE Trans. Commun.*, vol. 61, no. 8, pp. 3231–3245, 2013.

[106] J. Zhang and M. C. Gursoy, "Collaborative relay beamforming for secrecy," in *Commun. (ICC), 2010 IEEE Int. Conf.*, May 2010, pp. 1–5.

[107] H. M. Wang, M. Luo, X. G. Xia, and Q. Yin, "Joint cooperative beamforming and jamming to secure AF relay systems with individual power constraint and no eavesdropper's CSI," *IEEE Sig. Process. Lett.*, vol. 20, no. 1, pp. 39–42, 2013.

[108] K. H. Park, T. Wang, and M. S. Alouini, "On the jamming power allocation for secure amplify-and-forward relaying via cooperative jamming," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1741–1750, 2013.

[109] Y. Liu, L. Wang, T. T. Duy, M. Elkashlan, and T. Q. Duong, "Relay selection for security enhancement in cognitive relay networks," *IEEE Wireless Commun. Lett.*, vol. 4, no. 1, pp. 46–49, 2015.

[110] H. Hui, A. L. Swindlehurst, G. Li, and J. Liang, "Secure relay and jammer selection for physical layer security," *IEEE Sig. Process. Lett.*, vol. 22, no. 8, pp. 1147–1151, 2015.

[111] G. Geraci, M. Egan, J. Yuan, A. Razi, and I. B. Collings, "Secrecy sum-rates for multi-user MIMO regularized channel inversion precoding," *IEEE Trans. Commun.*, vol. 60, no. 11, pp. 3472–3482, 2012.

[112] M. P. Daly, E. L. Daly, and J. T. Bernhard, "Demonstration of directional modulation using a phased array," *IEEE Trans. Antennas Propag.*, vol. 58, no. 5, pp. 1545–1550, May 2010.

[113] A. Babakhani, D. B. Rutledge, and A. Hajimiri, "Transmitter architectures based on near-field direct antenna modulation," *IEEE J. Solid-State Circuits*, vol. 43, no. 12, pp. 2674–2692, 2008.

[114] ——, "A near-field modulation technique using antenna reflector switching," in *Solid-State Circuits Conf. 2008. ISSCC 2008. Dig. Technol. Pap. IEEE Int.*, 2008, pp. 188–605.

[115] R. M. Yamada, A. O. Steinhardt, and L. Mili, "Beamforming for simultaneous energy and information transfer and physical-layer secrecy," *IEEE Trans. Wireless Commun.*, vol. PP, no. 99, pp. 1–1, 2017.

[116] P. Shang, G. Zhu, L. Tan, G. Su, and T. Li, "Transmit antenna selection for the distributed MIMO systems," in *Networks Secur. Wireless Commun. Trust. Comput. 2009. NSWCTC '09. Int. Conf.*, vol. 2, 2009, pp. 449–453.

[117] H. Jin and J. Kim, "Combined antenna selection and beamforming for secure transmission in distributed antenna systems," in *ICT Converg. (ICTC), 2013 Int. Conf.*, 2013, pp. 1043–1047.

[118] J. M. Hamamreh, E. Güvenkaya, T. Baykas, and H. Arslan, "A practical physical-layer security method for precoded OSTBC-based systems," in *IEEE Wireless Commun. Netw. Conf., WCNC 2016, Doha, Qatar, Apr., 3-6*, 2016, pp. 1–6.

[119] N. Zhao, F. R. Yu, M. Jin, Q. Yan, and V. C. M. Leung, "Interference alignment and its applications: A survey, research issues, and challenges," *IEEE Commun. Surv. Tut.*, vol. 18, no. 3, pp. 1779–1803, thirdquarter 2016.

[120] N. Zhao, Y. Cao, R. Yu, Y. Chen, M. Jin, and V. Leung, "Artificial noise assisted secure interference networks with wireless power transfer," *IEEE Trans. Veh. Technol.*, vol. PP, no. 99, pp. 1–1, 2017.

[121] N. Zhao, F. R. Yu, M. Li, Q. Yan, and V. C. M. Leung, "Physical layer security issues in interference- alignment-based wireless networks," *IEEE Commun. Mag.*, vol. 54, no. 8, pp. 162–168, August 2016.

[122] C. Jeong, I. M. Kim, and D. I. Kim, "Joint secure beamforming design at the source and the relay for an amplify-and-forward MIMO untrusted relay system," *IEEE Trans. Sig. Process.*, vol. 60, no. 1, pp. 310–325, 2012.

[123] J. M. Hamamreh and H. Arslan, "Joint PHY/MAC layer security design using ARQ with MRC and null-space independent, PAPR-aware artificial noise in SISO systems," *IEEE Trans. Wireless Commun.*, pp. 1–1, 2018.

[124] A. Sheikholeslami, M. Ghaderi, H. Pishro-Nik, and D. Goeckel, "Energy-efficient secrecy in wireless networks based on random jamming," *IEEE Trans. Commun.*, vol. 65, no. 6, pp. 2522–2533, June 2017.

[125] R. Negi and S. Goel, "Secret communication using artificial noise," in *VTC-2005-Fall. 2005 IEEE 62nd Veh. Technol. Conf. 2005.*, vol. 3, 2005, pp. 1906–1910.

[126] S. Goel and R. Negi, "Secret communication in presence of colluding eavesdroppers," in *MILCOM 2005 - 2005 IEEE Mil. Commun. Conf.* IEEE, 2005, pp. 1–6.

[127] ——, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, jun 2008.

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

[129] H. Qin, Y. Sun, T.-H. Chang, X. Chen, C.-Y. Chi, M. Zhao, and J. Wang, "Power allocation and time-domain artificial noise design for wiretap OFDM with discrete inputs," *IEEE Trans. Wireless Commun.*, vol. 12, no. 6, pp. 2717–2729, Jun 2013.

[130] Y. Yang and B. Jiao, "Artificial noise strategy for single-antenna systems over multi-path fading channels," in *2015 Int. Wirel. Commun. Mob. Comput. Conf.* IEEE, aug 2015, pp. 96–101.

[131] W. Liu, M. Li, G. Ti, X. Tian, and Q. Liu, "Transmit filter and artificial noise aided physical layer security for ofdm systems," in *2016 8th Inter. Conf. Wirel. Commun. Sig. Process. (WCSP)*, Oct 2016, pp. 1–5.

[132] M. Hussain, Q. Du, L. Sun, and P. Ren, "Security protection over wireless fading channels by exploiting frequency selectivity," in *2016 8th International Conference on Wireless Communications Signal Processing (WCSP)*, Oct 2016, pp. 1–5.

[133] H. Qin, X. Chen, X. Zhong, F. He, M. Zhao, and J. Wang, "Joint power allocation and artificial noise design for multiuser wiretap OFDM channels," in *2013 IEEE Int. Conf. Commun.* IEEE, jun 2013, pp. 2193–2198.

[134] A. Tom, A. Sahin, and H. Arslan, "Suppressing alignment: joint PAPR and out-of-band power leakage reduction for OFDM-based systems," *IEEE Trans. Commun.*, vol. 64, no. 3, pp. 1100–1109, March 2016.

[135] E. Guvenkaya, A. Sahin, and H. Arslan, "N-continuous OFDM with CP alignment," in *MILCOM 2015 - 2015 IEEE Mil. Commun. Conf.*, Oct 2015, pp. 587–592.

[136] T. Akitaya, S. Asano, and T. Saba, "Time-domain artificial noise generation technique using time-domain and frequency-domain processing for physical layer security in MIMO-OFDM systems," in *2014 IEEE Int. Conf. Commun. Work. ICC 2014*. IEEE, Jun 2014, pp. 807–812.

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

[138] S. Gollakota and D. Katabi, "Physical layer wireless security made fast and channel independent," in *2011 Proceedings IEEE INFOCOM*, April 2011, pp. 1125–1133.

[139] S. Liu, Y. Hong, and E. Viterbo, "Artificial Noise Revisited," *IEEE Trans. Infor. Theory*, vol. 61, no. 7, pp. 3901–3911, 2015.

[140] ——, "Unshared secret key cryptography," *IEEE Trans. Wireless Commun.*, vol. 13, no. 12, pp. 6670–6683, Dec 2014.

[141] S. A. A. Fakoorian and A. L. Swindlehurst, "Solutions for the MIMO gaussian wiretap channel with a cooperative jammer," *IEEE Trans. Sig. Process.*, vol. 59, no. 10, pp. 5013–5022, 2011.

[142] A. Mukherjee and J. Huang, "Deploying multi-antenna energy-harvesting cooperative jammers in the MIMO wiretap channel," in *Sig., Syst. Comput. (ASILOMAR), 2012 Conf. Rec. Forty Sixth Asilomar Conf.*, 2012, pp. 1886–1890.

[143] N. Anand, S.-J. Lee, and E. W. Knightly, "STROBE: Actively securing wireless communications using zero-forcing beamforming," in *Proc. IEEE INFOCOM*, 2012, pp. 720–728.

[144] J. Huang and A. L. Swindlehurst, "Robust secure transmission in MISO channels based on worst-case optimization," *IEEE Trans. Sig. Process.*, vol. 60, no. 4, pp. 1696–1707, 2012.

[145] W. Li, M. Ghogho, B. Chen, and C. Xiong, "Secure communication via sending artificial noise by the receiver: Outage secrecy capacity/region analysis," *IEEE Commun. Lett.*, vol. 16, no. 10, pp. 1628–1631, October 2012.

[146] Q. Li, H. Song, and K. Huang, "Achieving secure transmission with equivalent multiplicative noise in MISO wiretap channels," *IEEE Commun. Lett.*, vol. 17, no. 5, pp. 892–895, May 2013.

[147] A. E. Shafie, Z. Ding, and N. Al-Dhahir, "Spatio-temporal artificial noise design for secure MISOSE-OFDM systems," in *2016 IEEE Global Commun. Conf. (GLOBECOM)*, Dec 2016, pp. 1–6.

[148] ——, "Hybrid spatio-temporal artificial noise design for secure MIMOME-OFDM systems," *IEEE Trans. Veh. Tech.*, vol. 66, no. 5, pp. 3871–3886, May 2017.

[149] M. Soltani and H. Arslan, "Randomized beamforming with generalized selection transmission for security enhancement in MISO wiretap channels," *IEEE Access*, vol. 6, pp. 5589–5595, 2018.

[150] E. Tekin and A. Yener, "Achievable rates for the general gaussian multiple access wire-tap channel with collective secrecy," *arXiv Prepr. cs/0612084*, 2006.

[151] E. Tekin, "The gaussian multiple access wire-tap channel: wireless secrecy and cooperative jamming," in *Inf. Theory Appl. Work. 2007*, 2007, pp. 404–413.

[152] L. Lai and H. E. Gamal, "The relay-eavesdropper channel: Cooperation for secrecy," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4005–4019, 2008.

[153] X. He and A. Yener, "Two-hop secure communication using an untrusted relay: A case for cooperative jamming," in *IEEE Glob. Telecommun. Conf. (GLOBECOM)*, 2008, pp. 1–5.

[154] ——, "Secure degrees of freedom for Gaussian channels with interference: Structured codes outperform gaussian signaling," in *IEEE Glob. Telecommun. Conf. (GLOBECOM)*, Nov 2009, pp. 1–6.

[155] J. Xie and S. Ulukus, "Secure degrees of freedom of the Gaussian wiretap channel with helpers," in *Commun. Control. Comput. (Allerton), 2012 50th Annu. Allert. Conf.*, 2012, pp. 193–200.

[156] Y. Liu, J. Li, and A. P. Petropulu, "Destination assisted cooperative jamming for wireless physical-layer security," *IEEE Trans. Inf. Forensics Secur.*, vol. 8, no. 4, pp. 682–694, 2013.

[157] Q. Xu, P. Ren, H. Song, and Q. Du, "Security-aware waveforms for enhancing wireless communications privacy in cyber-physical systems via multipath receptions," *IEEE Internet Things J.*, vol. PP, no. 99, pp. 1–1, 2017.

[158] A. Wiesel, Y. C. Eldar, and S. Shamai, "Zero-forcing precoding and generalized inverses," *IEEE Trans. Sig. Process.*, vol. 56, no. 9, pp. 4409–4418, 2008.

[159] E. R. X. Li, J. Hwu, "Using antenna array redundancy and channel diversity for secure wireless transmissions," *J. Commun.*, vol. 2, no. 3, pp. 24–32, May 2007.

[160] H. M. Wang, T. Zheng, and X. G. Xia, "Secure MISO wiretap channels with multiantenna passive eavesdropper: Artificial noise vs. artificial fast fading," *IEEE Trans. Wireless Commun.*, vol. 14, no. 1, pp. 94–106, Jan 2015.

[161] G. Zheng, I. Krikidis, J. Li, A. P. Petropulu, and B. Ottersten, "Improving physical layer secrecy using full-duplex jamming receivers," *IEEE Trans. Sig. Proc.*, vol. 61, no. 20, pp. 4962–4974, Oct 2013.

[162] Y. Hua, Q. Zhu, and R. Sohrabi, "Fundamental properties of full-duplex radio for secure wireless communications," *CoRR*, vol. abs/1711.10001, 2017.

[163] S. Goekceli, O. Cepheli, S. T. Basaran, G. K. Kurt, G. Dartmann, and G. Ascheid, "How effective is the artificial noise? real-time analysis of a PHY security scenario," in *2017 IEEE Globecom Workshops (GC Wkshps)*, Dec 2017, pp. 1–7.

[164] E. Tekin and A. Yener, "The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2735–2751, 2008.

[165] S. Ulukus and E. Ekrem, "Securing wireless communications at the physical layer," R. Liu and W. Trappe, Eds. Boston, MA: Springer US, 2010, ch. 7 Cooperative Secrecy in Wireless Communications, pp. 143–172.

[166] C. H. Bennett, G. Brassard, and J.-M. Robert, "Privacy amplification by public discussion," *SIAM Journal on Computing*, vol. 17, no. 2, pp. 210–229, 1988.

[167] U. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, May 1993.

[168] R. Ahlswede and I. Csiszar, "Common randomness in information theory and cryptography. I. secret sharing," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121–1132, Jul 1993.

[169] ——, "Common randomness in information theory and cryptography. II. CR capacity," *IEEE Trans. Inf. Theory*, vol. 44, no. 1, pp. 225–240, 1998.

[170] U. Maurer and S. Wolf, "Secret-key agreement over unauthenticated public channels-part I: definitions and a completeness result," *IEEE Trans. Inf. Theory*, vol. 49, no. 4, pp. 822–831, Apr 2003.

[171] ——, "Secret-key agreement over unauthenticated public channels-part II: the simulatability condition," *IEEE Trans. Inf. Theory*, vol. 49, no. 4, pp. 832–838, Apr 2003.

[172] ——, "Secret-key agreement over unauthenticated public channels-part III: privacy amplification," *IEEE Trans. Inf. Theory*, vol. 49, no. 4, pp. 839–851, Apr 2003.

[173] L. Gyongyosi, S. Imre, and H. V. Nguyen, "A survey on quantum channel capacities," *IEEE Commun. Surv. Tut.*, vol. PP, no. 99, pp. 1–1, 2018.

[174] L. Chen, S. Jordan, Y.-K. Liu, D. Moody, R. Peralta, R. Perlner, and D. Smith-Tone, "Report on post-quantum cryptography," National Institute of Standards and Technology, Tech. Rep., 2016.

[175] H. Koorapaty, A. Hassan, and S. Chennakeshu, "Secure information transmission for mobile radio," *IEEE Commun. Lett.*, vol. 4, no. 2, pp. 52–55, Feb 2000.

[176] T. Aono, K. Higuchi, T. Ohira, B. Komiyama, and H. Sasaoka, "Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels," *IEEE Trans. Antennas Propag.*, vol. 53, no. 11, pp. 3776–3784, Nov 2005.

[177] C. Ye, A. Reznik, G. Sternburg, and Y. Shah, "On the secrecy capabilities of ITU channels," in *2007 IEEE 66th Veh. Technol. Conf.* IEEE, Sep 2007, pp. 2030–2034.

[178] B. Azimi-Sadjadi, A. Kiayias, A. Mercado, and B. Yener, "Robust key generation from signal envelopes in wireless networks," in *Proceedings of the 14th ACM Conference on Computer and Communications Security*, ser. CCS '07. New York, NY, USA: ACM, 2007, pp. 401–410.

[179] T. Kitano, A. Kitaura, H. Iwai, and H. Sasaoka, "A private key agreement scheme based on fluactions of ber in wireless communications," in *The 9th Int. Conf. on Advanced Commun. Tech.*, vol. 3, Feb 2007, pp. 1495–1499.

[180] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy: Extracting a secret key from an unauthenticated wireless channel," in *Proc. of the 14th ACM Int. Conf. on Mobile Comput. and Netw.*, ser. MobiCom '08. New York, NY, USA: ACM, 2008, pp. 128–139.

[181] S. Jana, S. N. Premnath, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy, "On the effectiveness of secret key extraction from wireless signal strength in real environments," *ACM MobiCom*, vol. 12, no. 5, pp. 321—-332, 2009.

[182] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. Mandayam, "Information-theoretically secret key generation for fading wireless channels," *IEEE Trans. Inf. Forensics Secur.*, vol. 5, no. 2, p. 32, 2010.

[183] Y. Abdallah, M. Abdel Latif, M. Youssef, A. Sultan, and H. El Gamal, "Keys through ARQ: Theory and practice," *IEEE Trans. Inf. Forensics Secur.*, vol. 6, no. 3, pp. 737–751, Sep 2011.

[184] Y. E. H. Shehadeh, O. Alfandi, K. Tout, and D. Hogrefe, "Intelligent mechanisms for key generation from multipath wireless channels," in *2011 Wireless Telecommun. Symp. (WTS)*, April 2011, pp. 1–6.

[185] C. Ye, A. Reznik, and Y. Shah, "Extracting secrecy from jointly gaussian random variables," in *2006 IEEE Int. Symp. Inf. Theory*. IEEE, Jul 2006, pp. 2593–2597.

[186] T. Shimizu, H. Iwai, and H. Sasaoka, "Reliability-based sliced error correction in secret key agreement from fading channel," in *2010 IEEE Wireless Commun. Netw. Conf.* IEEE, Apr 2010, pp. 1–6.

[187] S. N. Premnath, S. Jana, J. Croft, P. L. Gowda, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy, "Secret key extraction from wireless signal strength in real environments," *IEEE Trans. Mobile Comput.*, vol. 12, no. 5, pp. 917–930, May 2013.

[188] N. Patwari, J. Croft, S. Jana, and S. K. Kasera, "High-rate uncorrelated bit extraction for shared secret key generation from channel measurements," *IEEE Trans. Mobile Comput.*, vol. 9, no. 1, pp. 17–30, Jan 2010.

[189] S. Althunibat, V. Sucasas, and J. Rodriguez, "A physical-layer security scheme by phase-based adaptive modulation," *IEEE Trans. Veh. Technol.*, vol. PP, no. 99, pp. 1–1, 2017.

[190] S. C. Draper and A. M. Sayeed, "Secret key generation through OFDM multipath channel," in *2011 45th Annu. Conf. Inf. Sci. Syst.* IEEE, Mar 2011, pp. 1–6.

[191] Q. Wang, H. Su, K. Ren, and K. Kim, "Fast and scalable secret key generation exploiting channel phase randomness in wireless networks," in *Proc. IEEE INFOCOM*, Apr 2011, pp. 1422–1430.

[192] W. Wang, H. Jiang, X. Xia, P. Mu, and Q. Yin, "A wireless secret key generation method based on chinese remainder theorem in FDD systems," *Science China Inf. Sciences*, vol. 55, no. 7, pp. 1605–1616, Jul 2012.

[193] C. Y. Wu, P. C. Lan, P. C. Yeh, C. H. Lee, and C. M. Cheng, "Practical physical layer security schemes for MIMO-OFDM systems using precoding matrix indices," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1687–1700, Sep. 2013.

[194] H. Liu, Y. Wang, J. Yang, and Y. Chen, "Fast and practical secret key extraction by exploiting channel response," in *Proc. IEEE INFOCOM*, April 2013, pp. 3048–3056.

[195] H. Li, X. Wang, and J.-Y. Chouinard, "Eavesdropping-resilient OFDM system using sorted subcarrier interleaving," *IEEE Trans. Wireless Commun.*, vol. 14, no. 2, pp. 1155–1165, Feb 2015.

[196] J. Zhang, A. Marshall, R. Woods, and T. Q. Duong, "Efficient key generation by exploiting randomness from channel responses of individual OFDM subcarriers," *IEEE Trans. Commun.*, vol. 64, no. 6, pp. 2578–2588, June 2016.

[197] J. Zhang, R. Woods, T. Q. Duong, A. Marshall, Y. Ding, Y. Huang, and Q. Xu, "Experimental study on key generation for physical layer

security in wireless communications," *IEEE Access*, vol. 4, pp. 4464–4477, 2016.

[198] W. Cheng, A. Xu, Y. Jiang, H. Wen, H. Song, K. Ouyang, and X. Zhu, "The realization of key extraction based on USRP and OFDM channel response," in *IEEE Conf. on Commun. and Netw. Security (CNS)*, Oct 2017, pp. 374–375.

[199] J. Zhang, A. Marshall, R. Woods, and T. Q. Duong, "Design of an OFDM physical layer encryption scheme," *IEEE Tran. Veh. Tech.*, vol. 66, no. 3, pp. 2114–2127, March 2017.

[200] A. Sayeed and A. Perrig, "Secure wireless communications: Secret keys through multipath," *ICASSP, IEEE Int. Conf. Acoust. Speech Signal Process. - Proc.*, pp. 3013–3016, Mar 2008.

[201] Y. Liu, S. C. Draper, and A. M. Sayeed, "Exploiting channel diversity in secret key generation from multipath fading randomness," *IEEE Trans. Inf. Forensics Secur.*, vol. 7, no. 5, pp. 1484–1497, 2012.

[202] Y. El Hajj Shehadeh, O. Alfandi, K. Tout, and D. Hogrefe, "Intelligent mechanisms for key generation from multipath wireless channels," in *2011 Wirel. Telecommun. Symp.*, Apr 2011, pp. 1–6.

[203] Y. El Hajj Shehadeh, O. Alfandi, and D. Hogrefe, "Towards robust key extraction from multipath wireless channels," *J. Commun. Networks*, vol. 14, no. 4, pp. 385–395, Aug 2012.

[204] H. Li, X. Wang, Y. Zou, and W. Hou, "Eavesdropping-resilient OFDM system using CSI-based dynamic subcarrier allocation," in *2013 IEEE 77th Veh. Technol. Conf. (VTC Spring)*, Jun 2013, pp. 1–5.

[205] J. Hou and G. Kramer, "Effective secrecy: Reliability, confusion and stealth," in *2014 IEEE Int. Symp. on Inf. Theory*, June 2014, pp. 601–605.

[206] A. Kitaura, H. Iwai, and H. Sasaoka, "A scheme of secret key agreement based on received signal strength variation by antenna switching in land mobile radio," in *9th Int. Conf. on Advanced Commun. Tech.*, vol. 3, Feb 2007, pp. 1763–1767.

[207] C. Chen and M. A. Jensen, "Secrecy extraction from increased randomness in a time-variant MIMO channel," in *IEEE Glob. Telecommun. Conf. (GLOBECOM)*, Nov 2009, pp. 1–6.

[208] J. W. Wallace and R. K. Sharma, "Automatic secret keys from reciprocal mimo wireless channels: Measurement and analysis," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 3, pp. 381–392, Sept 2010.

[209] K. Zeng, D. Wu, A. Chan, and P. Mohapatra, "Exploiting multiple-antenna diversity for shared secret key generation in wireless networks," in *Proc. IEEE INFOCOM*, 2010, pp. 1–9.

[210] H. M. Furqan, J. M. Hamamreh, and H. Arslan, "Secret key generation using channel quantization with SVD for reciprocal MIMO channels," in *2016 Int. Symp. Wirel. Commun. Syst.* IEEE, sep 2016, pp. 597–602.

[211] L. Lai, Y. Liang, and W. Du, "Cooperative key generation in wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 8, pp. 1578–1588, 2012.

[212] Q. Wang, K. Xu, and K. Ren, "Cooperative secret key generation from phase estimation in narrowband fading channels," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 9, pp. 1666–1674, October 2012.

[213] M. Wilhelm, I. Martinovic, and J. B. Schmitt, "Secure key generation in sensor networks based on frequency-selective channels," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1779–1790, September 2013.

[214] H. Zhou, L. M. Huie, and L. Lai, "Secret key generation in the two-way relay channel with active attackers," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 3, pp. 476–488, March 2014.

[215] H. Liu, J. Yang, Y. Wang, Y. J. Chen, and C. E. Koksal, "Group secret key generation via received signal strength: Protocols, achievable rates, and implementation," *IEEE Trans. Mobile Comput.*, vol. 13, no. 12, pp. 2820–2835, Dec 2014.

[216] C. D. T. Thai, J. Lee, and T. Q. S. Quek, "Physical-layer secret key generation with colluding untrusted relays," *IEEE Trans. Wirel. Commun.*, vol. 15, no. 2, pp. 1517–1530, 2016.

[217] H. M. Furqan, J. M. Hamamreh, and H. Arslan, "Secure communication via untrusted switchable decode-and-forward relay," in *13th Int. Wireless Commun. and Mobile Comput. Conf., IWCMC 2017, Valencia, Spain, June 26-30, 2017*, 2017, pp. 1333–1337.

[218] J. W. Wallace, C. Chen, and M. A. Jensen, "Key generation exploiting MIMO channel evolution: Algorithms and theoretical limits," in *2009 3rd European Conf. on Antennas and Propag.*, March 2009, pp. 1499–1503.

[219] I. Csiszar and P. Narayan, "Secrecy generation for multiple input multiple output channel models," in *2009 IEEE Int. Symp. on Inf. Theory*, June 2009, pp. 2447–2451.

[220] C. Chen and M. A. Jensen, "Random number generation from multipath propagation: MIMO-based encryption key establishment," in *IEEE Antennas and Propag. Society Int. Symp.*, June 2009, pp. 1–4.

[221] K. Ren, H. Su, and Q. Wang, "Secret key generation exploiting channel characteristics in wireless communications," *IEEE Wireless Commun.*, vol. 18, no. 4, pp. 6–12, August 2011.

[222] T. Shimizu, H. Iwai, and H. Sasaoka, "Physical-layer secret key agreement in two-way wireless relaying systems," *IEEE Trans. Inf. Forensics Secur.*, vol. 6, no. 3, pp. 650–660, 2011.

[223] K. Chen, B. B. Natarajan, and S. Shattil, "Secret key generation rate with power allocation in relay-based LTE-A networks," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 11, pp. 2424–2434, Nov 2015.

[224] A. Sheikholeslami, D. Goeckel, and H. Pishro-nik, "Artificial intersymbol interference (ISI) to exploit receiver imperfections for secrecy," in *2013 IEEE Inter. Symp. Info. Theory*, July 2013, pp. 2950–2954.

[225] A. Sheikholeslami, D. Goeckel, and H. Pishro-Nik, "Everlasting secrecy by exploiting non-idealities of the eavesdropper's receiver," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1828–1839, September 2013.

[226] ——, "Jamming based on an ephemeral key to obtain everlasting security in wireless environments," *IEEE Trans. Wirel. Commun.*, vol. 14, no. 11, pp. 6072–6081, Nov 2015.

[227] T. Allen, J. Cheng, and N. Al-Dhahir, "Secure space-time block coding without transmitter CSI," *IEEE Wirel. Commun. Lett.*, vol. 3, no. 6, pp. 573–576, Dec 2014.

[228] T. R. Dean and A. J. Goldsmith, "Physical-layer cryptography through massive MIMO," *IEEE Trans. Info. Theory*, vol. 63, no. 8, pp. 5419–5436, Aug 2017.

[229] C. Wang and H. M. Wang, "Physical layer security in millimeter wave cellular networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 8, pp. 5569–5585, Aug 2016.

[230] S. Vuppala, S. Biswas, and T. Ratnarajah, "An analysis on secure communication in millimeter/micro-wave hybrid networks," *IEEE Trans. Commun.*, vol. 64, no. 8, pp. 3507–3519, Aug 2016.

[231] Y. Ju, H. M. Wang, T. X. Zheng, Y. Zhang, Q. Yang, and Q. Yin, "Secrecy throughput maximization for millimeter wave systems with artificial noise," in *2016 IEEE 27th Annual Int. Symp. on Personal, Indoor, and Mobile Radio Commun. (PIMRC)*, Sept 2016, pp. 1–6.

[232] Y. Ju, H. M. Wang, T. X. Zheng, and Q. Yin, "Secure transmission with artificial noise in millimeter wave systems," in *2016 IEEE Wireless Commun. and Netw. Conf.*, April 2016, pp. 1–6.

[233] ——, "Secure transmissions in millimeter wave systems," *IEEE Trans. Commun.*, vol. 65, no. 5, pp. 2114–2127, May 2017.

[234] L. Wang, M. Elkashlan, T. Q. Duong, and R. W. Heath, "Secure communication in cellular networks: The benefits of millimeter wave mobile broadband," in *2014 IEEE 15th Int. Work. Sig. Process. Advances Wireless Commun. (SPAWC)*, June 2014, pp. 115–119.

[235] N. N. Alotaibi and K. A. Hamdi, "Silent antenna hopping transmission technique for secure millimeter-wave wireless communication," in *2015 IEEE Glob. Commun. Conf. (GLOBECOM)*, Dec 2015, pp. 1–6.

[236] ——, "A low-complexity antenna subset modulation for secure millimeter-wave communication," in *2016 IEEE Wireless Commun. Netw. Conf.*, April 2016, pp. 1–6.

[237] ——, "Switched phased-array transmission architecture for secure millimeter-wave wireless communication," *IEEE Trans. Commun.*, vol. 64, no. 3, pp. 1303–1312, March 2016.

[238] C. Chen, Y. Dong, X. Cheng, and N. Yi, "An iterative FFT-based antenna subset modulation for secure millimeter wave communications," in *2017 Int. Con. on Comp., Netw. Commun. (ICNC)*, Jan 2017, pp. 454–459.

[239] Y. Zhu, L. Wang, K. K. Wong, and R. W. Heath, "Secure communications in millimeter wave Ad Hoc networks," *IEEE Trans. Wireless Commun.*, vol. 16, no. 5, pp. 3205–3217, May 2017.

[240] Y. R. Ramadan and H. Minn, "Artificial noise aided hybrid precoding design for secure mmwave MISO systems with partial channel knowledge," *IEEE Sig. Proc. Lett.*, vol. 24, no. 11, pp. 1729–1733, Nov 2017.

[241] Y. R. Ramadan, H. Minn, and A. S. Ibrahim, "Hybrid analog-digital precoding design for secrecy mmwave MISO-OFDM systems," *IEEE Trans. Commun.*, vol. 65, no. 11, pp. 5009–5026, Nov 2017.

[242] X. Tian, M. Li, Z. Wang, and Q. Liu, "Hybrid precoder and combiner design for secure transmission in mmwave MIMO systems," in *GLOBECOM 2017 - IEEE Global Commun. Conf.*, Dec 2017, pp. 1–6.

[243] Y. Ju, H. M. Wang, T. X. Zheng, Q. Yin, and M. H. Lee, "Safeguarding millimeter wave communications against randomly located eavesdroppers," *IEEE Trans. Wirel. Commun.*, vol. PP, no. 99, pp. 1–1, 2018.

[244] S. Vuppala, Y. J. Tolossa, G. Kaddoum, and G. Abreu, "On the physical layer security analysis of hybrid millimeter wave networks," *IEEE Trans. Commun.*, vol. 66, no. 3, pp. 1139–1152, March 2018.

[245] Y. Zhang, H. M. Wang, Q. Yang, and Z. Ding, "Secrecy sum rate maximization in non-orthogonal multiple access," *IEEE Commun. Lett.*, vol. 20, no. 5, pp. 930–933, May 2016.

[246] Y. Li, M. Jiang, Q. Zhang, Q. Li, and J. Qin, "Secure beamforming in downlink MISO non-orthogonal multiple access systems," *IEEE Trans. Veh. Technol.*, vol. 66, no. 8, pp. 7563–7567, Aug 2017.

[247] M. Tian, Q. Zhang, S. Zhao, Q. Li, and J. Qin, "Secrecy sum rate optimization for downlink MIMO non-orthogonal multiple access systems," *IEEE Sign. Process. Lett.*, vol. 24, 2017.

[248] M. Jiang, Y. Li, Q. Zhang, Q. Li, and J. Qin, "Secure beamforming in downlink MIMO non-orthogonal multiple access networks," *IEEE Sig. Process. Lett.*, vol. 24, no. 12, pp. 1852–1856, Dec 2017.

[249] Y. Liu, Z. Qin, M. Elkashlan, Y. Gao, and L. Hanzo, "Enhancing the physical layer security of non-orthogonal multiple access in large-scale networks," *IEEE Trans. Wireless Commun.*, vol. 16, no. 3, pp. 1656–1672, March 2017.

[250] Z. Ding, Z. Zhao, M. Peng, and H. V. Poor, "On the spectral efficiency and security enhancements of NOMA assisted multicast-unicast streaming," *IEEE Trans. Commun.*, vol. 65, no. 7, pp. 3151–3163, July 2017.

[251] B. He, A. Liu, N. Yang, and V. K. N. Lau, "On the design of secure non-orthogonal multiple access systems," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 10, pp. 2196–2206, Oct 2017.

[252] H. Lei, J. Zhang, K. H. Park, P. Xu, I. S. Ansari, G. Pan, B. Alomair, and M. S. Alouini, "On secure NOMA systems with transmit antenna selection schemes," *IEEE Access*, vol. 5, pp. 17 450–17 464, 2017.

[253] D. Xu, P. Ren, Q. Du, L. Sun, and Y. Wang, "Combat eavesdropping by full-duplex technology and signal transformation in non-orthogonal multiple access transmission," in *2017 IEEE Int. Conf. Commun. (ICC)*, May 2017, pp. 1–6.

[254] O. Abbasi and A. Ebrahimi, "Secrecy analysis of a NOMA system with full duplex and half duplex relay," in *2017 Iran Work. on Commun. and Inf. Theory (IWCIT)*, May 2017, pp. 1–6.

[255] L. Lv, Q. Ni, Z. Ding, and J. Chen, "Cooperative non-orthogonal relaying for security enhancement in untrusted relay networks," in *2017 IEEE Int. Conf. Commun. (ICC)*, May 2017, pp. 1–6.

[256] S. Sinanovic, N. Serafimovski, M. D. Renzo, and H. Haas, "Secrecy capacity of space keying with two antennas," in *2012 IEEE Veh. Technol. Conf. (VTC Fall)*, Sept 2012, pp. 1–5.

[257] X. Guan, Y. Cai, and W. Yang, "On the secrecy mutual information of spatial modulation with finite alphabet," in *2012 Inter. Conf. Wireless Commun. and Sig. Proc. (WCSP)*, Oct 2012, pp. 1–4.

[258] S. R. Aghdam, T. M. Duman, and M. Di Renzo, "On secrecy rate analysis of spatial modulation and space shift keying," in *IEEE Int. Black Sea Conf. Commun. Netw.*, May 2015, pp. 63–67.

[259] L. Wang, S. Bashar, Y. Wei, and R. Li, "Secrecy enhancement analysis against unknown eavesdropping in spatial modulation," *IEEE Communications Letters*, vol. 19, no. 8, pp. 1351–1354, Aug 2015.

[260] S. Rezaei Aghdam and T. Duman, "Physical layer security for space shift keying transmission with precoding," *IEEE Wirel. Commun. Lett.*, vol. PP, no. 99, pp. 1–1, 2016.

[261] S. R. Aghdam and T. M. Duman, "Secure space shift keying transmission using dynamic antenna index assignment," in *IEEE Global Commun. Con. (GLOBECOM)*, Dec 2017, pp. 1–6.

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

[263] F. Wu, L. L. Yang, W. Wang, and Z. Kong, "Secret precoding-aided spatial modulation," *IEEE Commun. Lett.*, vol. 19, no. 9, pp. 1544–1547, Sept 2015.

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

[265] X. Wang, X. Wang, and L. Sun, "Spatial modulation aided physical layer security enhancement for fading wiretap channels," in *2016 8th Inter. Conf. Wireless Commun. Sig. Proc. (WCSP)*, Oct 2016, pp. 1–5.

[266] C. Liu, L. L. Yang, and W. Wang, "Secure spatial modulation with a full-duplex receiver," *IEEE Wireless Commun. Lett.*, vol. PP, no. 99, pp. 1–1, 2017.

[267] Y. Lee, H. Jo, Y. Ko, and J. Choi, "Secure index and data symbol modulation for OFDM-IM," *IEEE Access*, vol. 5, pp. 24 959–24 974, 2017.

[268] A. Mostafa and L. Lampe, "Physical-layer security for indoor visible light communications," in *2014 IEEE Int. Conf. Commun. (ICC)*, June 2014, pp. 3342–3347.

[269] ——, "Physical-layer security for MISO visible light communication channels," *IEEE J. Sel. Areas Commun*, vol. 33, no. 9, pp. 1806–1818, Sept 2015.

[270] ——, "Pattern synthesis of massive led arrays for secure visible light communication links," in *2015 IEEE Int. Conf. Commun. Work. (ICCW)*, June 2015, pp. 1350–1355.

[271] H. L. Minh, A. T. Pham, Z. Ghassemlooy, and A. Burton, "Secured communications-zone multiple input multiple output visible light communications," in *2014 IEEE Globecom Work. (GC Wkshps)*, Dec 2014, pp. 505–511.

[272] A. Mostafa and L. Lampe, "Securing visible light communications via friendly jamming," in *2014 IEEE Globecom Work. (GC Wkshps)*, Dec 2014, pp. 524–529.

[273] H. Zaid, Z. Rezki, A. Chaaban, and M. S. Alouini, "Improved achievable secrecy rate of visible light communication with cooperative jamming," in *2015 IEEE Global Conf. Sig. Inf. Process. (GlobalSIP)*, Dec 2015, pp. 1165–1169.

[274] T. V. Pham and A. T. Pham, "On the secrecy sum-rate of MU-VLC broadcast systems with confidential messages," in *2016 10th Int. Symp. Commun. Syst., Netw. and Digital Sig. Process. (CSNDSP)*, July 2016, pp. 1–6.

[275] A. Mostafa and L. Lampe, "Optimal and robust beamforming for secure transmission in MISO visible-light communication links," *IEEE Trans. Sig. Process.*, vol. 64, no. 24, pp. 6501–6516, Dec 2016.

[276] M. A. Arfaoui, Z. Rezki, A. Ghrayeb, and M. S. Alouini, "On the secrecy capacity of MISO visible light communication channels," in *2016 IEEE Glob. Commun. Conf. (GLOBECOM)*, Dec 2016, pp. 1–7.

[277] ——, "On the input distribution and optimal beamforming for the MISO VLC wiretap channel," in *2016 IEEE Glob. Conf. Sig. Inf. Process. (GlobalSIP)*, Dec 2016, pp. 970–974.

[278] X. Liu, X. Wei, L. Guo, Y. Liu, and Y. Zhou, "A new eavesdropping-resilient framework for indoor visible light communication," in *2016 IEEE Glob. Commun. Conf. (GLOBECOM)*, Dec 2016, pp. 1–6.

[279] H. Lu, L. Zhang, W. Chen, and Z. Wu, "Design and analysis of physical layer security based on ill-posed theory for optical OFDM-based VLC system over real-valued visible light channel," *IEEE Photon. J.*, vol. 8, no. 6, pp. 1–19, Dec 2016.

[280] B. Chen, L. Zhang, and H. Lu, "High security differential chaos-based modulation with channel scrambling for WDM-aided VLC system," *IEEE Photon. J*, vol. 8, no. 5, pp. 1–13, Oct 2016.

[281] Y. M. Al-Moliki, M. T. Alresheedi, and Y. Al-Harthi, "Secret key generation protocol for optical OFDM systems in indoor VLC networks," *IEEE Photon. J.*, vol. 9, no. 2, pp. 1–15, April 2017.

[282] H. Shen, Y. Deng, W. Xu, and C. Zhao, "Secrecy-oriented transmitter optimization for visible light communication systems," *IEEE Photon. J.*, vol. 8, no. 5, pp. 1–14, Oct 2016.

[283] S. Ma, Z. L. Dong, H. Li, Z. Lu, and S. Li, "Optimal and robust secure beamformer for indoor MISO visible light communication," *J. Lightw. Technol*, vol. 34, no. 21, pp. 4988–4998, Nov 2016.

[284] F. J. Lopez-Martinez, G. Gomez, and J. M. Garrido-Balsells, "Physical-layer security in free-space optical communications," *IEEE Photon. J.*, vol. 7, no. 2, pp. 1–14, April 2015.

[285] X. Sun and I. B. Djordjevic, "Physical-layer security in orbital angular momentum multiplexing free-space optical communications," *IEEE Photon. J.*, vol. 8, no. 1, pp. 1–10, Feb 2016.

[286] M. J. Saber and S. M. S. Sadough, "On secure free-space optical communications over malaga turbulence channels," *IEEE Wireless Commun. Lett.*, vol. 6, no. 2, pp. 274–277, April 2017.

[287] H. Endo, T. S. Han, T. Aoki, and M. Sasaki, "Numerical study on secrecy capacity and code length dependence of the performances in optical wiretap channels," *IEEE Photon. J.*, vol. 7, no. 5, pp. 1–18, Oct 2015.

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

[289] J. Wang, C. Liu, J. Wanga, Y. Wu, M. Lin, and J. Cheng, "Physical-layer security for indoor visible light communications: Secrecy capacity analysis," *IEEE Trans. Commun.*, pp. 1–1, 2018.

[290] M. Soltani and Z. Rezki, "Optical wiretap channel with input-dependent gaussian noise under peak-and average-intensity constraints," *IEEE Trans. Info. Theory*, pp. 1–1, 2018.

[291] X. Zhao, H. Chen, and J. Sun, "On physical-layer security in multiuser visible light communication systems with non-orthogonal multiple access," *IEEE Access*, vol. 6, pp. 34 004–34 017, 2018.

[292] E. K. Lee, M. Gerla, and S. Y. Oh, "Physical layer security in wireless smart grid," *IEEE Commun. Mag.*, vol. 50, no. 8, pp. 46–52, August 2012.

[293] A. Pittolo and A. M. Tonello, "Physical layer security in PLC networks: Achievable secrecy rate and channel effects," in *2013 IEEE 17th Int. Symp. on Power Line Commun. and Its Appl.*, March 2013, pp. 273–278.

[294] ——, "Physical layer security in power line communication networks: an emerging scenario, other than wireless," *IET Commun.*, vol. 8, no. 8, pp. 1239–1247, May 2014.

[295] Y. Zhuang and L. Lampe, "Physical layer security in MIMO power line communication networks," in *18th IEEE Int. Symp. on Power Line Commun. and Its Appl.*, March 2014, pp. 272–277.

[296] A. Salem, K. M. Rabie, K. A. Hamdi, E. Alsusa, and A. M. Tonello, "Physical layer security of cooperative relaying power-line communication systems," in *2016 Int. Symp. on Power Line Commun. and its Appl. (ISPLC)*, March 2016, pp. 185–189.

[297] Y. J. Yoon, J. W. Choi, S. C. Kim, J. H. Lee, and Y. H. Kim, "The optimal power allocation for security in multicarrier relay power line communication," in *2016 Int. Symp. on Power Line Commun. and its Appl. (ISPLC)*, March 2016, pp. 190–195.

[298] A. E. Shafie, D. Niyato, R. Hamila, and N. Al-Dhahir, "Impact of the wireless network's PHY security and reliability on demand-side management cost in the smart grid," *IEEE Access*, vol. PP, no. 99, pp. 1–1, 2017.

[299] S. Liu, M. Ma, Y. Li, Y. Chen, and B. Jiao, "An absolute secure wireline communication method against wiretapper," *IEEE Commun. Lett.*, vol. 21, no. 3, pp. 536–539, March 2017.

[300] A. Elsamadouny, A. E. Shafie, M. Abdallah, and N. Al-Dhahir, "Secure sum-rate-optimal MIMO multicasting over medium-voltage NB-PLC networks," *IEEE Tran. Smart Grid*, vol. PP, no. 99, pp. 1–1, 2017.

[301] A. Mukherjee, "Physical-layer security in the internet of things: Sensing and communication confidentiality under resource constraints," *Proc. IEEE*, vol. 103, no. 10, 2015.

[302] Q. Xu, P. Ren, H. Song, and Q. Du, "Security enhancement for IoT communications exposed to eavesdroppers with uncertain locations," *IEEE Access*, vol. 4, pp. 2840–2853, 2016.

[303] B. Chen, C. Zhu, L. Shu, M. Su, J. Wei, V. C. M. Leung, and J. J. P. C. Rodrigues, "Securing uplink transmission for lightweight single-antenna ues in the presence of a massive mimo eavesdropper," *IEEE Access*, vol. 4, pp. 5374–5384, 2016.

[304] L. Brilli, T. Pecorella, and L. Mucchi, "Physical layer security for IoT devices configuration and key management - a proof of concept," in *2016 AEIT Int. Annual Conf. (AEIT)*, Oct 2016, pp. 1–6.

[305] G. Epiphaniou, P. Karadimas, D. K. B. Ismail, H. Al-Khateeb, A. Dehghantanha, and K. K. R. Choo, "Non-reciprocity compensation combined with turbo codes for secret key generation in vehicular ad hoc social IoT networks," *IEEE Internet Things J.*, vol. PP, no. 99, pp. 1–1, 2017.

[306] A. Soni, R. Upadhyay, and A. Jain, "Internet of things and wireless physical layer security: A survey," in *Computer Communication, Networking and Internet Security*, S. C. Satapathy, V. Bhateja, K. S. Raju, and B. Janakiramaiah, Eds. Singapore: Springer Singapore, 2017, pp. 115–123.

[307] L. Brilli, T. Pecorella, and L. Mucchi, "Physical layer security for iot devices configuration and key management - a proof of concept," in *2016 AEIT Inter. Ann. Conf. (AEIT)*, Oct 2016, pp. 1–6.

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

[309] M. Rushanan, A. D. Rubin, D. F. Kune, and C. M. Swanson, "Sok: Security and privacy in implantable medical devices and body area networks," in *Proc. of the 2014 IEEE Symp. on Secur. and Privacy*, ser. SP '14. Washington, DC, USA: IEEE Computer Society, 2014, pp. 524–539.

[310] G. Zheng, R. Shankaran, M. A. Orgun, L. Qiao, and K. Saleem, "Ideas and challenges for securing wireless implantable medical devices: A review," *IEEE Sensors J.*, vol. 17, no. 3, pp. 562–576, Feb 2017.

[311] K. Malasri and L. Wang, "Securing wireless implantable devices for healthcare: Ideas and challenges," *IEEE Commun. Mag.*, vol. 47, no. 7, pp. 74–80, July 2009.

[312] T. Halevi and N. Saxena, "Acoustic eavesdropping attacks on constrained wireless device pairing," *IEEE Trans. Inf. Forensics Secur.*, vol. 8, no. 3, pp. 563–577, March 2013.

[313] S. Gollakota, H. Hassanieh, B. Ransford, D. Katabi, and K. Fu, "They can hear your heartbeats: Non-invasive security for implantable medical devices," *SIGCOMM Comput. Commun. Rev.*, vol. 41, no. 4, pp. 2–13, Aug. 2011.

[314] H. Niu, L. Sun, M. Ito, and K. Sezaki, "Secure transmission through multihop relaying in wireless body area networks," in *2014 IEEE 3rd Glob. Conf. on Consumer Electronics (GCCE)*, Oct 2014, pp. 395–396.

[315] S. T. Ali, V. Sivaraman, D. Ostry, G. Tsudik, and S. Jha, "Securing first-hop data provenance for body-worn devices using wireless link fingerprints," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 12, pp. 2193–2204, Dec 2014.

[316] S. T. Ali, V. Sivaraman, and D. Ostry, "Eliminating reconciliation cost in secret key generation for body-worn health monitoring devices," *IEEE Trans. Mobile Comput.*, vol. 13, no. 12, pp. 2763–2776, Dec 2014.

[317] R. Dautov and G. R. Tsouri, "Securing while sampling in wireless body area networks with application to electrocardiography," *IEEE J. Biomed. Health Inform*, vol. 20, no. 1, pp. 135–142, Jan 2016.

[318] Z. Zhang, H. Wang, A. V. Vasilakos, and H. Fang, "Channel information based cryptography and authentication in wireless body area networks," in *Proc. of the 8th Int. Conf. Body Area Netw.*, ser. BodyNets '13. ICST, Brussels, Belgium, Belgium: ICST (Institute for Computer Sciences, Social-Inform. and Telecommun. Engin.), 2013, pp. 132–135.

[319] Z. Li and H. Wang, "A key agreement method for wireless body area networks," in *2016 IEEE Conf. on Computer Commun. Work. (INFOCOM Wkshps)*, April 2016, pp. 690–695.

[320] H. Moosavi and F. M. Bui, "Delay-aware optimization of physical layer security in multi-hop wireless body area networks," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 9, pp. 1928–1939, Sept 2016.

[321] B. Mokhtar and M. Azab, "Survey on security issues in vehicular ad hoc networks," *Alexandria Engin. J.*, vol. 54, no. 4, pp. 1115 – 1126, 2015.

[322] J. Wan, A. B. Lopez, and M. A. A. Faruque, "Exploiting wireless channel randomness to generate keys for automotive cyber-physical system security," in *2016 ACM/IEEE 7th Int. Conf. on Cyber-Physical Syst. (ICCPS)*, April 2016, pp. 1–10.

[323] M. E. Eltayeb, J. Choi, T. Y. Al-Naffouri, and R. W. Heath, "Enhancing secrecy with multi-antenna transmission in millimeter wave vehicular communication systems," *IEEE Trans. Veh. Technol.*, vol. PP, no. 99, pp. 1–1, 2017.

[324] Y. O. Basciftci, F. Chen, J. Weston, R. Burton, and C. E. Koksal, "How vulnerable is vehicular communication to physical layer jamming attacks?" in *2015 IEEE 82nd Veh. Technol. Conf. (VTC2015-Fall)*, Sept 2015, pp. 1–5.

[325] X. Zhu, F. Xu, E. Novak, C. C. Tan, Q. Li, and G. Chen, "Using wireless link dynamics to extract a secret key in vehicular scenarios," *IEEE Trans. Mobile Comput.*, vol. 16, no. 7, pp. 2065–2078, July 2017.

[326] A. M. Salih Abdelgader, S. Feng, and L. Wu, "Exploiting the randomness inherent of the channel for secret key sharing in vehicular communications," *Int. J. Intell. Transp. Syst. Research*, vol. 16, no. 1, pp. 39–50, Jan 2018.

[327] H. Sakran, M. Shokair, O. Nasr, S. El-Rabaie, and A. El-Azm, "Proposed relay selection scheme for physical layer security in cognitive radio networks," *IET Commun.*, vol. 6, pp. 2676–2687, Nov. 2012.

[328] W. Li, M. Xin, M. Yue, T. Yinglei, and Z. Yong, "Security-oriented transmission based on cooperative relays in cognitive radio," *China Commun.*, vol. 10, no. 8, pp. 27–35, Aug 2013.

[329] Y. Zou, B. Champagne, W. P. Zhu, and L. Hanzo, "Relay-selection improves the security-reliability trade-off in cognitive radio systems," *IEEE Trans. Commun. Technol.*, vol. 63, no. 1, pp. 215–228, Jan 2015.

[330] C. Wang and H. M. Wang, "On the secrecy throughput maximization for MISO cognitive radio network in slow fading channels," *IEEE Trans. Inf. Forensics Secur.*, vol. 9, no. 11, pp. 1814–1827, Nov 2014.

[331] Y. Zou, X. Li, and Y. C. Liang, "Secrecy outage and diversity analysis of cognitive radio systems," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 11, pp. 2222–2236, Nov. 2014.

[332] Y. Zou, X. Wang, and W. Shen, "Physical-layer security with multiuser scheduling in cognitive radio networks," *IEEE Trans. Commun. Technol.*, vol. 61, no. 12, pp. 5103–5113, Dec. 2013.

[333] W. Jiang and W. Feng, "Cognitive radio network secure communication with and without cooperative jammer," in *2014 Int. Conf. on Advanced Technol. for Commun. (ATC 2014)*, Oct 2014, pp. 621–626.

[334] T. Zhang, Y. Huang, Y. Cai, C. Zhong, W. Yang, and G. K. Karagiannidis, "Secure multi-antenna cognitive wiretap networks," *IEEE Trans. Veh. Technol.*, vol. 66, no. 5, pp. 4059–4072, May 2017.

[335] W. Yang, K. Wang, X. Xu, and J. Zhou, "Secure transmission for AF relaying spectrum-sharing systems with collaborative distributed beamforming," in *2016 25th Wireless and Opt. Commun. Conf. (WOCC)*, May 2016, pp. 1–4.

[336] N. Zhang, N. Lu, N. Cheng, J. W. Mark, and X. S. Shen, "Cooperative spectrum access towards secure information transfer for CRNs," *IEEE J. Sel. Areas Commun*, vol. 31, no. 11, pp. 2453–2464, Nov. 2013.

[337] Y. He, J. Evans, and S. Dey, "Secrecy rate maximization for cooperative overlay cognitive radio networks with artificial noise," in *2014 IEEE Int. Conf. on Commun. (ICC)*, June 2014, pp. 1663–1668.

[338] I. Stanojev and A. Yener, "Improving secrecy rate via spectrum leasing for friendly jamming," *IEEE Trans. Wireless Commun.*, vol. 12, no. 1, pp. 134–145, January 2013.

[339] D. Wang, P. Ren, Y. Wang, Q. Du, and L. Sun, "Cooperative jamming with untrusted SUs for secure communication of two-hop primary system," in *2015 Int. Wireless Commun. and Mobile Comput. Conf. (IWCMC)*, Aug 2015, pp. 90–95.

[340] D. Wang, P. Ren, Q. Du, L. Sun, and Y. Wang, "Cooperative relaying and jamming for primary secure communication in cognitive two-way networks," in *2016 IEEE 83rd Veh. Tech. Conf. (VTC Spring)*, May 2016, pp. 1–5.

[341] Q. Gao, Y. Huo, L. Ma, X. Xing, X. Cheng, T. Jing, and H. Liu, "Optimal stopping theory based jammer selection for securing cooperative cognitive radio networks," in *2016 IEEE Glob. Commun. Conf. (GLOBECOM)*, Dec 2016, pp. 1–6.

[342] Y. Pei, Y. C. Liang, L. Zhang, K. C. Teh, and K. H. Li, "Achieving cognitive and secure transmissions using multiple antennas," in *2009 IEEE 20th Annual Int. Symp. on Personal, Indoor, and Mobile Radio Commun. (PIMRC)*, Sept 2009, pp. 1–5.

[343] Y. Pei, Y. c. Liang, L. Zhang, K. C. Teh, and K. H. Li, "Secure communication over MISO cognitive radio channels," *IEEE Trans. Wireless Commun.*, vol. 9, no. 4, pp. 1494–1502, April 2010.

[344] P. Yan, Y. Zou, and J. Zhu, "Transmit antenna selection to improve physical layer security for MIMO-CR systems," in *2016 8th Int. Conf. Wireless Commun. Sig. Process. (WCSP)*, Oct 2016, pp. 1–4.

[345] H. Lei, M. Xu, I. S. Ansari, G. Pan, K. A. Qaraqe, and M. S. Alouini, "On secure underlay MIMO cognitive radio networks with energy harvesting and transmit antenna selection," *IEEE Trans. Green Commun. Netw.*, vol. 1, no. 2, pp. 192–203, June 2017.

[346] F. Alavi, N. Mokari, and H. Saeedi, "Secure resource allocation in OFDMA-based cognitive radio networks with two-way relays," in *2015 23rd Iranian Conf. Elect. Eng.*, May 2015, pp. 171–176.

[347] W. Saad, Z. Han, and H. V. Poor, "On the physical layer security of backscatter RFID systems," in *2012 Int. Symp. on Wireless Commun. Syst. (ISWCS)*, Aug 2012, pp. 1092–1096.

[348] W. Saad, X. Zhou, Z. Han, and H. V. Poor, "On the physical layer security of backscatter wireless systems," *IEEE Trans. Wireless Commun.*, vol. 13, no. 6, pp. 3442–3451, June 2014.

[349] Q. Yang, Y. Zhang, H. M. Wang, and Z. Han, "Transmit optimization for secure MIMO RFID wireless communication," in *2016 IEEE Int. Conf. Commun. (ICC)*, May 2016, pp. 1–6.

[350] Q. Yang, H. M. Wang, Y. Zhang, and Z. Han, "Physical layer security in MIMO backscatter wireless systems," *IEEE Trans. Wireless Commun.*, vol. 15, no. 11, pp. 7547–7560, Nov 2016.

[351] H. Hassanieh, J. Wang, D. Katabi, and T. Kohno, "Securing RFIDs by randomizing the modulation and channel," in *NSDI*, 2015.

[352] V. B. Suresh and W. P. Burleson, "Reflex: Reconfigurable logic for entropy extraction," in *2014 27th IEEE Int. System-on-Chip Conf. (SOCC)*, Sept 2014, pp. 341–346.

[353] F. Marino, E. Paolini, and M. Chiani, "Secret key extraction from a UWB channel: Analysis in a real environment," in *2014 IEEE Int. Conf. Ultra-WideBand (ICUWB)*, Sept 2014, pp. 80–85.

[354] M. G. Madiseh, M. L. McGuire, S. W. Neville, and A. A. B. Shirazi, "Secret key extraction in ultra wideband channels for unsynchronized radios," in *6th Annual Commun. Netw. Serv. Research Conf. (cnsr 2008)*, May 2008, pp. 88–95.

[355] M. Ko and D. L. Goeckel, "Wireless physical-layer security performance of UWB systems," in *2010 IEEE Military Commun. Conf. (MILCOM)*, Oct 2010, pp. 2143–2148.

[356] A. Hennessy and A. Alimohammad, "Design and implementation of a digital secure code-shifted reference UWB transmitter and receiver," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 64, no. 7, pp. 1927–1936, July 2017.

[357] D. B. Ha, N. G. Nguyen, D. D. Tran, and T. H. Nguyen, "Physical layer security in UWB communication systems with transmit antenna selection," in *2014 Int. Conf. Comput., Manag. and Telecommun. (ComManTel)*, April 2014, pp. 280–285.

[358] J. Yue, C. Ma, H. Yu, and W. Zhou, "Secrecy-based access control for device-to-device communication underlaying cellular networks," *IEEE Commun. Lett.*, vol. 17, no. 11, pp. 2068–2071, Nov. 2013.

[359] D. Zhu, A. L. Swindlehurst, S. A. A. Fakoorian, W. Xu, and C. Zhao, "Device-to-device communications: The physical layer security advantage," in *2014 IEEE Int. Conf. Acoust., Speech Sig. Process. (ICASSP)*, May 2014, pp. 1606–1610.

[360] W. Shen, W. Hong, X. Cao, B. Yin, D. M. Shila, and Y. Cheng, "Secure key establishment for device-to-device communications," in *2014 IEEE Glob. Commun. Conf. GLOBCOM*, Dec 2014, pp. 336–340.

[361] R. Zhang, X. Cheng, and L. Yang, "Joint power and access control for physical layer security in D2D communications underlaying cellular networks," in *2016 IEEE Int. Conf. Commun. (ICC)*, May 2016, pp. 1–6.

[362] ——, "Cooperation via spectrum sharing for physical layer security in device-to-device communications underlaying cellular networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 8, pp. 5651–5663, Aug 2016.

[363] J. Qu, Y. Cai, and S. Xu, "Power allocation in a secure-aware device-to-device communication underlaying cellular network," in *2016 8th Int. Conf. Wireless Commun. Sig. Process. (WCSP)*, Oct 2016, pp. 1–5.

[364] S. Yan, Y. Shang, X. Zhang, D. Li, and X. Li, "An artificial noise scheme for secure communication in heterogeneous D2D and cellular networks," in *2016 IEEE 84th Veh. Technol. Conf. (VTC-Fall)*, Sept 2016, pp. 1–5.

[365] R. Atat and L. Liu, "On the achievable transmission capacity of secrecy-based D2D cellular networks," in *2016 IEEE Glob. Commun. Conf. (GLOBECOM)*, Dec 2016, pp. 1–6.

[366] L. Sun, Q. Du, P. Ren, and Y. Wang, "Two birds with one stone: Towards secure and interference-free D2D transmissions via constellation rotation," *IEEE Trans. Veh. Technol.*, vol. 65, no. 10, pp. 8767–8774, Oct 2016.

[367] J. Wang, Q. Tang, C. Yang, R. Schober, and J. Li, "Security enhancement via device-to-device communication in cellular networks," *IEEE Signal Process. Lett.*, vol. 23, no. 11, pp. 1622–1626, Nov 2016.

[368] W. Mei, Z. Chen, J. Fang, and B. Fu, "Secure D2D-enabled cellular communication against selective eavesdropping," in *2017 IEEE Int. Conf. Commun. (ICC)*, May 2017, pp. 1–7.

[369] W. Mei, Z. Chen, and J. Fang, "Sum secrecy rate optimization for MIMOME wiretap channel with artificial noise and D2D underlay communication," in *2017 IEEE Int. Conf. Commun. (ICC)*, May 2017, pp. 1–7.

[370] A. Zhang and X. Lin, "Security-aware and privacy-preserving D2D communications in 5G," *IEEE Netw.*, vol. 31, no. 4, pp. 70–77, July 2017.

[371] M. Alibeigi, A. Taherpour, and S. Gazor, "Optimization of secrecy rate in cooperative device-to-device communications," in *2017 IEEE 30th Canadian Conf. on Elec. Computer Eng. (CCECE)*, April 2017, pp. 1–5.

[372] J. Ouyang, M. Lin, W. P. Zhu, K. An, and L. Wang, "Improving secrecy performance via device-to-device jamming in cellular networks," in *2016 8th Int. Conf. Wireless Commun. Sig. Process. (WCSP)*, Oct 2016, pp. 1–5.

[373] F. Alavi, N. M. Yamchi, M. R. Javan, and K. Cumanan, "Limited feedback scheme for device-to-device communications in 5G cellular networks with reliability and cellular secrecy outage constraints," *IEEE Trans. Veh. Technol.*, vol. 66, no. 9, pp. 8072–8085, Sept 2017.

[374] X. Kang, X. Ji, K. Huang, and Z. Zhong, "Secure D2D communication underlying cellular networks: Artificial noise assisted," in *2016 IEEE 84th Veh. Technol. Conf. (VTC-Fall)*, Sept 2016, pp. 1–5.

[375] J. Oh, Y. Kwon, and T. Hwang, "Energy-efficient link adaptation for secure D2D underlaid cellular networks," in *2016 IEEE Glob. Commun. Conf. (GLOBECOM)*, Dec 2016, pp. 1–6.

[376] Y. Kwon, H. Suh, J. Oh, and T. Hwang, "Energy efficient communication for secure D2D underlaid cellular networks," *IEEE Trans. Veh. Technol.*, vol. 66, no. 10, pp. 9110–9123, Oct 2017.

[377] H. Song, J. Y. Ryu, W. Choi, and R. Schober, "Joint power and rate control for device-to-device communications in cellular systems," *IEEE Trans. Wireless Commun.*, vol. 14, no. 10, pp. 5750–5762, Oct 2015.

[378] Y. Wu, J. Zheng, K. Guo, L. P. Qian, X. Shen, and Y. Cai, "Joint traffic scheduling and resource allocations for traffic offloading with secrecy provisioning," *IEEE Trans. Veh. Technol.*, vol. 66, no. 9, pp. 8315–8332, Sept 2017.

[379] C. Ma, J. Liu, X. Tian, H. Yu, Y. Cui, and X. Wang, "Interference exploitation in D2D-enabled cellular networks: A secrecy perspective," *IEEE Trans. Commun.*, vol. 63, no. 1, pp. 229–242, Jan 2015.

[380] K. Zhang, M. Peng, P. Zhang, and X. Li, "Secrecy-optimized resource allocation for device-to-device communication underlaying heterogeneous networks," *IEEE Trans. Veh. Technol.*, vol. 66, no. 2, pp. 1822–1834, Feb 2017.

[381] Q. Wang, Z. Chen, W. Mei, and J. Fang, "Improving physical layer security using UAV-enabled mobile relaying," *IEEE Wireless Commun. Lett.*, vol. 6, no. 3, pp. 310–313, June 2017.

[382] X. Qi, B. Li, Z. Chu, K. Huang, and H. Chen, "Secrecy energy efficiency analysis of UAV-enabled communication networks," *CoRR*, vol. abs/1704.01883, 2017.

[383] G. Zhang, Q. Wu, M. Cui, and R. Zhang, "Securing UAV communications via trajectory optimization," *arXiv preprint arXiv:1710.04389*, 2017.

[384] T. Rappaport, R. Heath, R. Daniels, and J. Murdock, *Millimeter wave wireless communications*. Prentice Hall, 2015, includes bibliographical references (pages 585-651) and index.

[385] Z. Lin, M. Lin, J. B. Wang, Y. Huang, and W. P. Zhu, "Robust secure beamforming for 5G cellular networks coexisting with satellite networks," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 932–945, April 2018.

[386] W. Q. Wang and Z. Zheng, "Hybrid MIMO and phased-array directional modulation for physical layer security in mmwave wireless communications," *IEEE J. Sel. Areas Commun.*

[387] W. Liang, Z. Ding, and H. V. Poor, *Non-Orthogonal Multiple Access (NOMA) for 5G Systems*. Cambridge University Press, 2017, p. 109132.

[388] X. Chen, Z. Zhang, C. Zhong, D. W. K. Ng, and R. Jia, "Exploiting inter-user interference for secure massive non-orthogonal multiple access," *CoRR*, vol. abs/1802.07926, 2018.

[389] E. Basar, M. Wen, R. Mesleh, M. D. Renzo, Y. Xiao, and H. Haas, "Index modulation techniques for next-generation wireless networks," *IEEE Access*, vol. 5, no. 1, pp. 16 693–16 746, Sep. 2017.

[390] M. Wen, X. Cheng, and L. Yang, *Index Modulation for 5G Wireless Communications*. Springer International Publishing, 2017.

[391] X. Q. Jiang, M. Wen, H. Hai, J. Li, and S. Y. Kim, "Secrecy-enhancing scheme for spatial modulation," *IEEE Commun. Lett.*, vol. PP, no. 99, pp. 1–1, 2017.

[392] H. Taha and E. Alsusa, "Secret key exchange and authentication via randomized spatial modulation and phase shifting," *IEEE Trans. Veh. Technol.*, vol. PP, no. 99, pp. 1–1, 2017.

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

[394] S. Arnon, *Visible Light Communication*, 1st ed. New York, NY, USA: Cambridge University Press, 2015.

[395] A. Mukherjee, "Secret-key agreement for security in multi-emitter visible light communication systems," *IEEE Commun. Lett.*, vol. 20, no. 7, pp. 1361–1364, July 2016.

[396] B. I., B. G., D. A., L. R., M. A., and S. A., *PLC for Smart Grid*. Wiley-Blackwell, 2016, ch. 9, pp. 509–561.

[397] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," *IEEE Commun. Surv. Tut.*, vol. 17, no. 4, pp. 2347–2376, Fourthquarter 2015.

[398] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1125–1142, Oct 2017.

[399] R. Cavallari, F. Martelli, R. Rosini, C. Buratti, and R. Verdone, "A survey on wireless body area networks: Technologies and design challenges," *IEEE Commun. Surv. Tut.*, vol. 16, no. 3, pp. 1635–1657, Third 2014.

[400] C. Cooper, D. Franklin, M. Ros, F. Safaei, and M. Abolhasan, "A comparative survey of VANET clustering techniques," *IEEE Commun. Sur. Tut.*, vol. 19, no. 1, pp. 657–681, Firstquarter 2017.

[401] X. Wang, Z. Ning, and L. Wang, "Offloading in internet of vehicles: A fog-enabled real-time traffic management system," *IEEE Trans Ind. Informat.*, pp. 1–1, 2018.

[402] Z. Ning, X. Wang, X. Kong, and W. Hou, "A social-aware group formation framework for information diffusion in narrowband internet of things," *IEEE Internet of Things Journal*, vol. 5, no. 3, pp. 1527–1538, June 2018.

[403] Z. Ning, F. Xia, N. Ullah, X. Kong, and X. Hu, "Vehicular social networks: Enabling smart mobility," *IEEE Commun. Mag.*, vol. 55, no. 5, pp. 16–55, May 2017.

[404] Z. Ning, X. Hu, Z. Chen, M. Zhou, B. Hu, J. Cheng, and M. S. Obaidat, "A cooperative quality-aware service access system for social internet of vehicles," *IEEE Internet of Things Journal*, pp. 1–1, 2017.

[405] Z. Ning, F. Xia, X. Hu, Z. Chen, and M. S. Obaidat, "Social-oriented adaptive transmission in opportunistic internet of smartphones," *IEEE Trans Ind. Informat.*, vol. 13, no. 2, pp. 810–820, April 2017.

[406] T. Yucek and H. Arslan, "A survey of spectrum sensing algorithms for cognitive radio applications," *IEEE Commun. Surv. Tut.*, vol. 11, no. 1, pp. 116–130, First 2009.

[407] F. Hu, B. Chen, and K. Zhu, "Full spectrum sharing in cognitive radio networks toward 5G: A survey," *IEEE Access*, vol. 6, pp. 15 754–15 776, 2018.

[408] M. Amjad, M. H. Rehmani, and S. Mao, "Wireless multimedia cognitive radio networks: A comprehensive survey," *IEEE Commun. Surv. Tut.*, vol. 20, no. 2, pp. 1056–1103, Secondquarter 2018.

[409] Y. Cao, N. Zhao, F. R. Yu, M. Jin, Y. Chen, J. Tang, and V. C. M. Leung, "Optimization or alignment: Secure primary transmission assisted by secondary networks," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 905–917, April 2018.

[410] V. Niemel, J. Haapola, M. Hmlinen, and J. Iinatti, "An ultra wideband survey: Global regulations and impulse radio research based on standards," *IEEE Commun. Surv. Tut.*, vol. 19, no. 2, pp. 874–890, Secondquarter 2017.

[411] A. Asadi, Q. Wang, and V. Mancuso, "A survey on device-to-device communication in cellular networks," *IEEE Commun. Surv. Tut.*, vol. 16, no. 4, pp. 1801–1819, Fourthquarter 2014.

[412] P. Gandotra, R. K. Jha, and S. Jain, "A survey on device-to-device (D2D) communication: Architecture and security issues," *Journal of Network and Computer Applications*, vol. 78, pp. 9 – 29, 2017.

[413] S. Hayat, E. Yanmaz, and R. Muzaffar, "Survey on unmanned aerial vehicle networks for civil applications: A communications viewpoint," *IEEE Commun. Surv. Tut.*, vol. 18, no. 4, pp. 2624–2661, Fourthquarter 2016.

[414] L. Gupta, R. Jain, and G. Vaszkun, "Survey of important issues in UAV communication networks," *IEEE Commun. Surv. Tut.*, vol. 18, no. 2, pp. 1123–1152, Secondquarter 2016.

[415] M. H. Yilmaz, E. Guvenkaya, H. M. Furqan, S. Kose, and H. Arslan, "Cognitive security of wireless communication systems in the physical," *Wireless Commun. Mobile Comput.*, 2017.

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

[417] P. Huang and X. Wang, "Fast secret key generation in static wireless networks: A virtual channel approach," in *Proc. IEEE INFOCOM*, April 2013, pp. 2292–2300.

[418] D. Chen, Z. Qin, X. Mao, P. Yang, Z. Qin, and R. Wang, "Smokegrenade: An efficient key generation protocol with artificial interference," *IEEE Trans. Info. Forensics Security*, vol. 8, no. 11, pp. 1731–1745, Nov 2013.

[419] R. Guillaume, S. Ludwig, A. Mller, and A. Czylwik, "Secret key generation from static channels with untrusted relays," in *2015 IEEE 11th Inter. Conf. Wireless Mob. Comp. Netw. Commun. (WiMob)*, Oct 2015, pp. 635–642.

[420] S. Sharifian, F. Lin, and R. Safavi-Naini, "Secret key agreement using a virtual wiretap channel," in *IEEE INFOCOM 2017 - IEEE Conf. Computer Commun.*, May 2017, pp. 1–9.

[421] G. Li, A. Hu, J. Zhang, and B. Xiao, "Security analysis of a novel artificial randomness approach for fast key generation," in *GLOBECOM 2017 - 2017 IEEE Global Commun. Conf.*, Dec 2017, pp. 1–6.

[422] Y. Ding, J. Zhang, and V. F. Fusco, "Retrodirective-assisted secure wireless key establishment," *IEEE Trans. Commun.*, vol. 65, no. 1, pp. 320–334, Jan 2017.

[423] P. Viswanath, D. N. C. Tse, and R. Laroia, "Opportunistic beamforming using dumb antennas," *IEEE Trans. Info. Theory*, vol. 48, no. 6, pp. 1277–1294, Jun 2002.

[424] T. Hong and Z. P. Li, "Peak-to-average power ratio reduction for an artificial noise aided secure communication system," in *2016 3rd Inter. Conf. Infor. Sci. Cont. Eng. (ICISCE)*, July 2016, pp. 1370–1374.

[425] J. Qiao, H. Zhang, X. Zhou, and D. Yuan, "Joint beamforming and time switching design for secrecy rate maximization in wireless-powered FD relay systems," *IEEE Trans. Veh. Technol.*, vol. PP, no. 99, pp. 1–1, 2017.

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