Received: 9 November 2020 | Revised: 29 January 2021 | Accepted: 9 March 2021

DOI: 10.1002/ett.4270

SURVEY PAPER

WILEY

A comprehensive survey of physical layer security over fading channels: Classifications, applications, and challenges

Poonam Yadav[1] | **Sandeep Kumar**[2] | **Rajesh Kumar**[1]

[1]Department of Electronics and Communication, NERIST, Nirjuli, India

[2]Central Research Laboratory, BEL, Ghaziabad, Uttar Pradesh, 201010, India

Correspondence
Sandeep Kumar, Central Research Laboratory, BEL, Ghaziabad, Uttar Pradesh, 201010, India.
Email: sann.kaushik@gmail.com

Abstract

Due to the open nature of wireless communication systems, the data transmission over these networks are vulnerable to malicious attack. To safeguard the transmitted data, physical layer security (PLS) has been emerged as a promising technique because of its unique feature of utilizing randomness of the wireless channel to secure the information. The preeminent idea of utilizing the channel imperfections such as fading and noise into the security providing resource is the basic approach behind PLS. For exploiting the randomness of the propagation medium, the analysis of the secrecy performance over the fading channel is of utmost importance. With the explanation of basic theory and technology, this paper presents an elaborated survey on the PLS research over the fading channels. To exploit the performance gains, we discuss the optimization approaches in different network design problems, for example, secrecy rate maximization, power minimization, and secure energy efficiency problems. We present a comparative study of the expressions of various performance metrics of the PLS along with classification depending upon the channel state information of the eavesdropper. The application and challenges of the PLS in the emerging wireless technologies are also reviewed and discussed. This paper incorporates almost all the aspects of PLS implemented over the fading channels. Furthermore, the paper is concluded with open research directions for the PLS system in various fields that can be explored to design a flexible and robust security system to satisfy the security requirements of the next-generation networks.

1 | INTRODUCTION

Wireless communications have become a vital part of the present world's daily life and the data transfer over these networks are increasing for a wide range of applications such as military applications, banking and financial transactions, and social networking, and so on.[1] With the exponential growth in wireless services, information security has become a prime issue, as people rely on the wireless network for the transmission of confidential information. Moreover, because of the broadcasting nature of the wireless medium, it is considered to be potentially unsafe. In the wireless transmission, any sufficiently close ED can detect the broadcast information and possibly intercept/decode the transmitted signals or

generate jamming for disrupting legitimate transmissions.[2] Information security techniques are essential to ensure the secure delivery of information over these networks.

Traditionally, information security technologies rely on cryptographic approach to ensure confidentiality and authenticity of the data.[3] In the cryptographic technique, the confidential message which is required to be transmitted is encrypted using some encryption algorithm alongside a secret key that is shared only with the legitimate receiver.[4] At the receiving end, only the legitimate receiver can decrypt this message with the help of the pre-shared secret key.[5] Due to the advancement in computational methodologies, there is a chance that this encrypted text can still be decrypted by the ED, launching a brute force attack.[6] Physical layer security (PLS) is an alternative paradigm to provide security in wireless networks from malicious attacks. Unlike, cryptographic, PLS is implemented on the physical layer of the network architecture and exploits any form of physical characteristics of the propagation medium to provide security.[7] Considering the scenario of the services offered by the next generation network PLS is a preferable technique over cryptographic approach. The main reason for it is 3-fold. First, the next-generation networks[8] are heterogeneous network which is multilevel and have weak architecture, so management and distribution of the secret keys become extremely difficult. Second, these networks are expected to support diverse services, such as cashless transactions, web browsing, social networking, and so on and each service has diverse security requirements. For instance, in cashless transaction services, security guarantee must be tighter than the other applications. Encryption-based method can only provide binary security level, so there are numerous risks, as advanced computing capabilities can bring disastrous threat to the network. So, the service-oriented and user-driven security trust cannot be accomplished using cryptographic technique. Third, in the services like IoT or M2M communication devices with limited computing capabilities, storage, and power resource are incorporated, so it is cumbersome to apply the complicated enc/dec security technique over these devices.

The PLS provides a promising solution to the above discussed and many more limitations with emerging wireless applications. It has several advantages over the cryptographic techniques. For instance, PLS does not rely on the enc/dec algorithms, thus overcomes the difficulty of distribution and management of secret keys in heterogeneous networks, which are decentralized. In PLS, adaptive signal design and resource allocation is actualized relying upon the physical attributes of the channel hence it provides flexible security to the diverse wireless applications.

As the PLS approach of secure communication does not rely on computational complexity, so even if the ED is loaded with equipment with high computing capabilities, secure and reliable communication can still be achieved. The concept of the PLS is thoroughly explained by the authors in References 9,10 and in Figure 1 the comparison of the cryptographic security approach and PLS approach is illustrated.

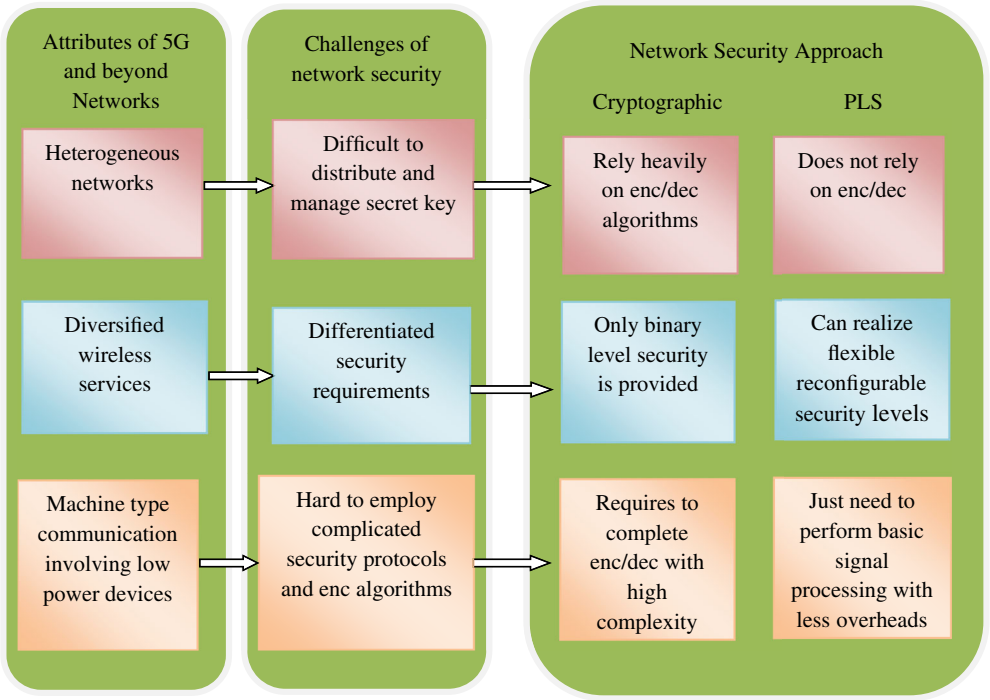
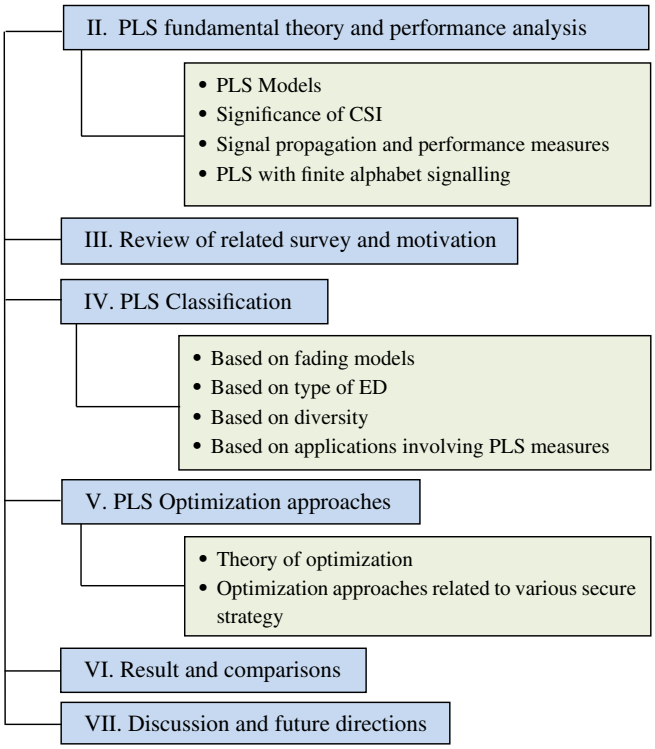


FIGURE 1 Comparison of cryptographic security and PLS approach

FIGURE 2 Outline and framework of the survey



PLS requires the legitimate transmitter and receiver to have the advantage over the ED in terms of channel quality, which cannot be guaranteed in the practical communication system. However, this limitation of the PLS is reduced with arrival of enabling technologies such as MIMO systems, smart antennas and devices with high computational capabilities.[11] Since the basic idea behind PLS is to exploit the randomness of the propagation medium, this survey presents a complete detail of the PLS work over various fading channels. The main objective of this paper is to present a unified framework that can incorporate all the PLS enabling work performed over the fading channels in the presence of the active and passive ED under one roof. The major contribution of this survey paper can be summarized as follows:

- Review of the state-of-the-art results on PLS, this paper provides a comprehensive technical discussion to facilitate and inspire future research in the analysis, design, optimization, and implementation of the physical security of wireless networks.
- An in-depth description of fundamental terminology, performance metrics, different scenarios, architectures, and contributions from the up-to-date works of PLS over various fading models. Comparisons, advantages and limitations of the performance analysis, computational complexity, implementation constraints, and generalization of the derived expressions and techniques over fading channels.
- To shed light on the significance of implementing PLS in the emerging next-generation wireless applications to satisfy the security prerequisites and constraints by utilizing the specific characteristics of these applications.
- To review the optimization of secure resource allocation, beamforming/precoding, antenna/node selection, and cooperation strategies in PLS. This is followed with usually appeared optimization approaches to enhance the system performance.
- Open challenges which highlight the limitations of the current literature are analyzed. The technical insights and way ahead in terms of executions of the application scenarios, architectures, and technologies are explored.

The organization of this paper proceeds as follows. In Section 2 the concept of PLS, including the system model along with the performance measurements are explained. In Section 3, a review of the existing PLS survey paper is performed. Section 4 presents the classification of the PLS based on fading channels, ED, diversity and, the PLS implementation on emerging applications. Section 5 comprises of the review of various optimization approaches used in PLS systems. In Section 6, results and comparisons are demonstrated. Section 7 consists of the discussion over the future directions and finally ends with a conclusion in Section 8. A systematic framework and outline of this survey is provided in Figure 2. Tables 1 and 2 are provided with abbreviations and symbols used throughout this work.

TABLE 1 List of abbreviations

AAG	Active antenna group
AF	Amplify and forward
AN	Artificial noise
AP	Access point
ASC	Average secrecy capacity
ASOP	Alternative secrecy outage probability
AWGN	Additive White Gaussian noise
BAN	Body area network
CSI	Channel state information
CSIT	Channel state information at transmitter
CGR	Channel gain ratio
CR	Cognitive radio
D2D	Device-to-device
DEC	Decryption
DF	Decode and forward
ED	Eavesdropper
EGBFHF	Extended generalized bivariate Fox H function
EGBMGF	Extended generalized bivariate Meijer G function
EGC	Equal gain combining
EH	Energy harvesting
ENC	Encryption
ESC	Ergodic secrecy capacity
eMBB	Enhanced mobile broadband
FDA	Frequency diverse array
FSO	Free space optical
GSOP	Generalized secrecy outage probability
GSVD	Generalized singular value decomposition
HPPP	Homogeneous Poisson point processes
IG	Inverse gamma
i.i.d.	Independent and identically distributed
i.n.i.d.	Independent and non-identically distributed
IoT	Internet of things
IRS	Intelligent reflecting surfaces
JPAC	Joint power and access control
LDPC	Low-density parity check
LED	Light emitting diode
LN	Lognormal
LPDA	Log periodic dual dipole antenna
LTE	Long term evolution
MIMO	Multiple input multiple output
MIMOME	Multiple input multiple output multiantenna eavesdropper

(Continues)

TABLE 1 (Continued)

MISO	Multiple input single output
ML	Machine learning
MoG	Mixture of gamma
M2M	Machine-to-machine
MRC	Maximal ratio combining
mMTC	Massive machine type communication
mm-WAVE	Millimeter-wave
NOMA	Non-orthogonal multiple access
OFDM	Orthogonal frequency division multiplexing
OFDMA	Orthogonal frequency division multiple access
PCC	Power correlation coefficient
PLS	Physical layer security
PNZ	Probability of non-zero secrecy capacity
PSK	Phase shift keying
QAM	Quadrature amplitude modulation
QoS	Quality of services
RF	Radio frequency
SCA	Successive convex approximation
SDP	Semi-definite programming
SISO	Single input single output
SISOME	Single input single output multiantenna eavesdropper
SINR	Signal-interference-noise ratio
SNR	Signal-to-noise ratio
SOP	Secrecy outage probability
SOP^{L}	Lower bound SOP
SPSC	Strictly positive secrecy capacity
SR	Secrecy rate
SWIPT	Simultaneous wireless information and power transfer
RSS	Random subcarrier selection
UAV	Unmanned ariel vehicle
URLLC	Ultra-reliable low latency communication
VANET	Vehicular adhoc network
V2V	Vehicle-to-vehicle
VLC	Visible light communication
ZF	Zero forcing
5G	Fifth generation

TABLE 2 List of symbols

C_s	Secrecy capacity
C_B	Capacity of Bob
C_E	Capacity of Eve
γ_B	SNR of Bob
γ_E	SNR of Eve
γ_{th}	Threshold SNR
h_{AB}	Channel co-efficient of Bob
h_{AE}	Channel co-efficient of Eve
σ_B^2	Channel noise power of Bob
σ_E^2	Channel noise power of Eve
R_s	Secrecy rate
R_L	Information leakage rate
Δ	Fractional equivocation
$\overline{\Delta}$	Average fractional equivocation
$\mathbb{E}\{.\}$	Expectation operator
P_e	Decoding error probability

2 | PLS FUNDAMENTALS: THEORY AND PERFORMANCE ANALYSIS

2.1 | PLS models

The idea behind the PLS was first conceptualized by Shannon.[12] Shannon's cipher model considered a noiseless system where a transmitter communicates with a legitimate receiver in the presence of an ED. The model assumed that a random key is shared among the transmitter and the legitimate receiver and that key is also known to the ED. According to this, system achieves perfect secrecy if the entropy of the secret key surpasses the entropy of the message. Shannon's cipher system considered a very stringent secrecy standard, as it requires statistical autonomy between the transmitted message and the channel output at ED. Unlike Shannon, Wyner proposed a wiretap model in Reference 13, which takes the advantage of the degraded feature of the wireless channel to provide security without the need of a secret key. The resulting model uses a wiretap channel, as shown in Figure 3. Wyner wiretap channel model is composed of a legitimate transmitter known as Alice, which tries to communicate a message M to the legitimate receiver known as Bob in the presence of an ED called as Eve. Eve tries to intercept the transmission through the other noisy channel. The channel between Alice and Bob is called as main channel, and the channel intercepted by Eve is called as a wiretap channel. The message M is encoded into code word X^n of the length n and sent over the main channel with a rate R_s. At the receiving end, Bob and Eve try to track the same message by decoding their received code as Y^n and Z^n, respectively. R_s is said to achieve secrecy rate if reliability condition, $\lim_{n\to\infty} P_r(\widehat{M} \neq M) = 0$ and secrecy condition, $\lim_{n\to\infty} I(M; Z^n) = 0$ are satisfied. These conditions guarantee that as $n \to \infty$, decoding error probability at the Bob is arbitrarily small, and no source data are acquired at the ED. Here, $\widehat{M}$ is the estimated message received at Bob and $I(M; Z^n)$ is the mutual information between M and Z^n. The maximum attainable secrecy rate is defined as the SC, which portrays the constraints of the rate for secure transmission in the noisy channel. For a degraded wiretap channel, SC is mathematically given as

$$C_s = \max_{p(x)} (I(M; Y) - I(M; Z)) \tag{1}$$

where $p(x)$ is the probabilistic distribution of the input M at the transmitter. The channel quality of the main link is represented by the mutual information term, $I(M; Y)$. It also describes the rate at which Alice can transmit to Bob. Similarly, $I(M; Z)$ is the channel quality between Alice and Eve. For getting a positive secrecy capacity, the main channel has to be less noisy than the wiretap channel. From the expression, it is clear that for secure transmission rate, SC should be at

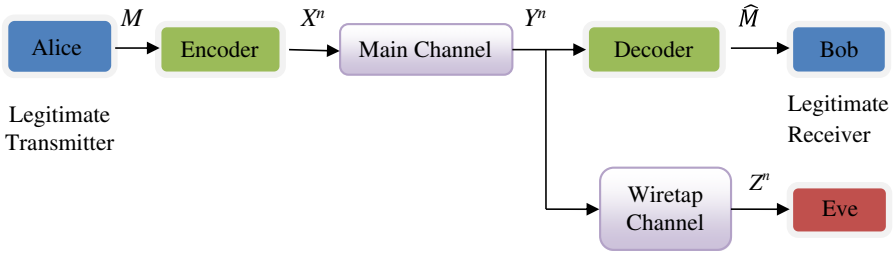


FIGURE 3 Generic model of wiretap channel

least or more than the difference between the capacities at legitimate receiver and ED. This concludes that Alice and Bob must have a favorable position at the physical layer itself. The results presented by Wyner was generalized by the authors in Reference 14 considering a general independent system condition and studied transmission by eliminating degraded ED channel assumption.

2.2 | Significance of CSI in PLS

The unique feature of fading model is that it utilizes randomness of the channel gain to provide secure transmission from the ED at the physical layer itself. So, even if the SNR of ED is better than the legitimate channel, PLS can be still achieved without the need of sharing the secret key.[15-17] To fully benefit from what the fading has to provide, CSI at the transmitter is of primordial importance. The assumption of perfect CSIT reduces the complexity of the secrecy analysis and allows the characterization of the full potential of the fading wiretap channel but it does not capture the practicality of the transmission system. Specifically, in the case of passive Eve, it is far away from the possibility as the sole interest of passive Eve is to only intercept the data transmission between Alice and Bob. This is usually obtained prior to data transmission by the feedback received from the receiver in the practical wireless communication system. A vast majority of works assume that the transmitter has a perfect knowledge of the CSI of both the main and the ED channels or at least of the main channel. In Reference 18, a synopsis of how different levels of CSI at the transmitter impact the system's security is presented. Similarly, Reference 19 presents a survey on PLS under the CSI assumption, with a particular focus on relay channels, cognitive systems, and large-scale decentralized networks. The channel links over which this feedback information is sent can be either noisy, rate-limited, or delayed leading to CSIT uncertainty. In Reference 20, authors have comprehensively review PLS with perfect CSIT, partial CSIT, main CSIT uncertainty, and no CSIT. The perfect CSIT is the case when Alice has the CSI of both Bob and Eve whereas in partial CSIT only the CSI of Bob is known.[16,21-23] In wireless communication, different phenomena cause the CSI to be imperfect. The uncertainty in the CSI comes from the error of estimation at the transmitter which can lead to the noisy version of the CSI or due to the delayed feedback causing outdated CSI. In this area, some exhaustive works can be found in the literature.[24-27] In the case of sensor and ad-hoc networks, channel variation is fast so the receiver becomes unable to estimate it and feedback to the transmitter. In such cases, transmitter transmits on the basis of the statistics available at the main and ED channel. The ergodic SC over the fast fading channel under the no CSI assumption is analyzed in Reference 28 considering different stochastic orders. This illustration is presented for the Nakagami-*m* channel and has shown that the proposed achievable secrecy scheme can outperform the Gaussian codebook in several cases. An exact expression to analyze SC over the fast fading Rayleigh fading channel under no CSI is derived in Reference 29. The block fading Rayleigh channel of MIMO system under the no CSI is examined in Reference 30. The secure degree of freedom is analyzed and proved that as long as ED has lesser antenna than the legitimate receiver, a positive secure degree of freedom can be achieved for a constant norm channel input. Some more work on PLS under no CSI assumption can be found in the literatures.[31,32]

As per the above discussions, it is clear that to achieve the optimal performance of the secure transmission, the perfect CSI of both legitimate and the ED channel is indispensable for system design. Conventionally, to obtain the CSI, training is performed in the forward direction by having Alice emit pilot signals at the beginning of each coherence interval to enable channel estimation at Bob. Channel feedback is then sent from Bob to Alice and then the confidential data is transmitted, as shown in Figure 4. Since these schemes make no attempt to prevent CSI leakage to Eve, they are often devised by assuming perfect CSI at Eve, and thus are suitable for worst-case scenarios.[18] However, due to the existence of estimation error and feedback delay in some cases, it may be difficult in practice to get the perfect CSI of the legitimate channel.

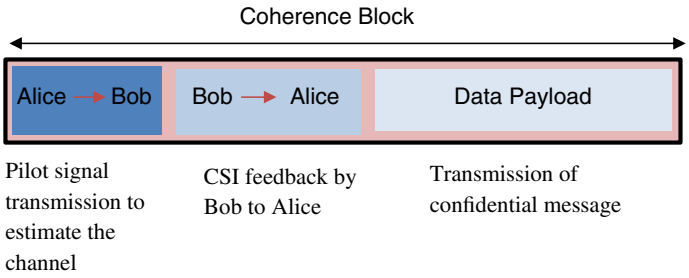


FIGURE 4 CSI transmission and feedback over a coherence block

By capitalizing on training in the reverse direction (ie, from Bob to Alice), several techniques have been proposed in the literature to prevent such (Alice-Eve) CSI leakage. Reverse training can be viewed as an intelligent way to perform channel estimation and feedback simultaneously without benefiting the ED.[33,34] In the cases where perfect CSI of the wiretap channel is unknown, imperfect CSI of the wiretap channel can have obtained based on the past channel observation or prior knowledge of the propagation environment.[35] Apart from these, there are certain situations where the ED is not at all known to the legitimate transmitter, as taken in Reference 30. In this, for a MIMO Rayleigh fading channel where neither training nor feedback is applied, and thus, no instantaneous CSI is available at any node. A constant norm channel input is proposed to exploit the non-coherent nature of the channel and is shown to achieve the optimal performance at high SNR. In Reference 36, authors have proposed a power control strategy that does not require the transmitter to transmit pilot signal for the estimation of the channel or to feedback the estimated channel to the receiver. In this, the transmitter varies the power and phase of the transmitted signal as per channel to the receiver, such that receiver can decode the information without having CSI. This eliminates the requirement of the feedback from transmitter to receiver, which helps in hiding the transmitter and achieves covert communication. Similarly, References 37,38 also investigate covert communication system under block fading channels where transceivers have uncertainty on the related CSI. From the review of the various literatures, we conclude that knowledge of the CSI is highly correlated with the achievable SR. It depicts that more the transmitter is having the knowledge of CSI better is the SR.

2.3 | Signal propagation and performance measures

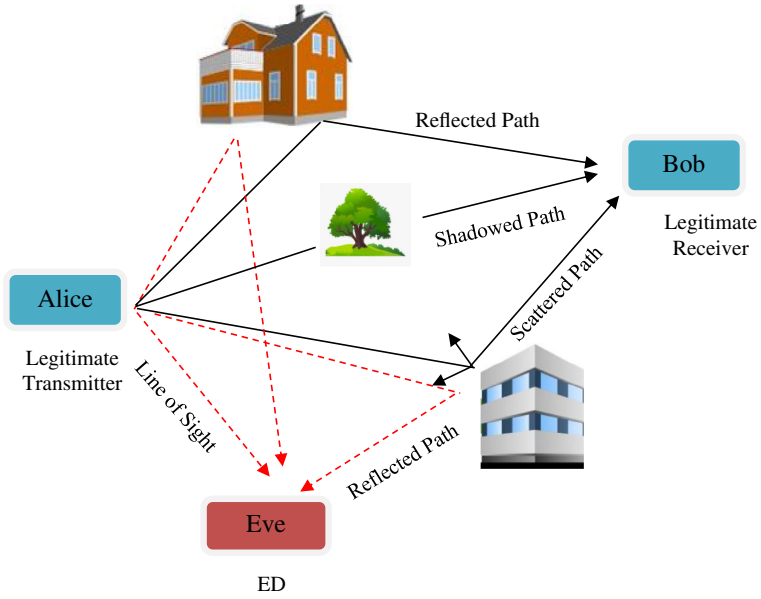
The information-theoretic security approach can be extended to model the physical wireless channel. Wireless PLS is one of the key applications of the concept explained in the previous section, as the imperfections of the wireless medium can help to establish the security of the communication system.[39] Figure 5 below shows the practical wireless propagation scenario with the ED who is trying to intercept the main channel. The legitimate transmitter, Alice transmits a signal which experiences multiple propagations due to channel impairments such as reflection, scattering, shadowing which, leads to the degradation of the signal at Bob and Eve. This phenomenon is termed as fading. The multiple effects produced by the channel on the transmitted signal are called as the channel gain and is represented by the multiplicative variable. An extension of the Wyner model, using the Gaussian wiretap channel, is provided in Reference 11, which is the most basic model used to account for the PLS of the wireless channel. At moment t, the legitimate transmitter Alice sends a signal $x(t)$ to the Bob, whereas Eve is trying to overhear, the received signal at Bob $r_b(t)$ and at Eve $r_e(t)$ is given as

$$r_b(t) = h_{AB}(t) + n_B(t)$$

$$r_e(t) = h_{AE}(t) + n_E(t) \tag{2}$$

where n_B and n_E are the AWGN component of the receiver and the ED, respectively. The channel coefficient can be estimated by any channel model available to represent the randomness of the wireless channel. SNR is a significant parameter to estimate the channel quality. This ratio provides the estimation, how strong is the data signal power as compared to non-data signal power which is occurring due to the channel noise and interference. For the evaluation of the secrecy performance of a given system, some numerical metrics have been adopted or developed from the conventional communication metric such as channel capacity, SNR, and BER. The various performance metrics used to analyze the PLS over the wireless channel are expressed in the terms of the instantaneous received SNR. Following are the classification of the performance metrics of the PLS system.

FIGURE 5 Wireless propagation scenario with ED



2.3.1 | Secrecy capacity

It is defined as the difference between the capacities of the main channel and the ED channel. As per the definition the secrecy capacity C_s is formulated as given in Reference 16.

$$C_s = \max(C_B - C_E, 0) \tag{3}$$

A useful measure of the channel quality is SNR, as it provides information on how strong is the received data. Let γ_B be the instantaneous received SNR at the legitimate receiver B and γ_E be the instantaneous received SNR at the ED. The SC is given as

$$C_s = \max(log_2(1 + \gamma_B) - log_2(1 + \gamma_E), 0) \tag{4}$$

where, $\gamma_B = P_{signal}|h_{AB}|^2/{\sigma_B}^2$ and $\gamma_E = P_{signal}|h_{AE}|^2/{\sigma_E}^2$, in which h_{AB} and h_{AE} are the channel coefficient of legitimate and the wiretap channel respectively. P_{signal} is the average transmit power. ${\sigma_B}^2$, and ${\sigma_E}^2$ are the channel noise power of the legitimate user and the ED, respectively. Under this condition, secure transmission can occur if the legitimate link has better SNR than the wiretap link. The expression of the secrecy capacity is given as

$$C_s = \begin{cases} log_2(1 + \gamma_B) - log_2(1 + \gamma_E) & \gamma_B > \gamma_E \\ 0 & \gamma_B \leq \gamma_E \end{cases} \tag{5}$$

2.3.2 | Secrecy outage probability

It is characterized as the probability that the instantaneous SC falls below the predefined secrecy rate. Mathematically expressed as

$$SOP = P_{out} = P_r(C_s(\gamma_B, \gamma_E) < R_s) \tag{6}$$

where R_s is the predefined secrecy rate, which is defined in terms of threshold SNR γ_{th}. When the CSI of Eve is unknown to the Alice in that case, Alice transmits the information at a constant secrecy rate. As long as the $C_s > R_s$, Eve's channel will be worse than Bob's, and secure transmission will take place otherwise, the security is compromised. A dedicated analysis

of SOP is presented in the literature.[40-42] In some typical fading channel conditions, the expression of SOP becomes very complex to analyze so SOP^L is analyzed to get the insights of the system, expressed as

$$SOP \geq SOP^L = P_r(\gamma_B/\gamma_E < 2^{R_s}) \tag{7}$$

In context to this, to assess the PLS performance over the fading channel work is proposed in the literature.[43-45] In spite of the convenience of the customary SOP in assessing the security performance of wireless channels, it has three fundamental limitations. To start with, it comes up short on the capability to quantitatively describe the measure of the information leakage to the EDs when secrecy outage occurs. Second, it cannot give any bit of knowledge on the ED's ability to effectively decoding the secret messages. Third, it cannot be connected with the QoS requirements of various applications, and services. Motivated by these facts, authors in Reference 46 proposed three new metrics dependent on the distribution of fractional equivocation. These metrics include generalized SOP, average fractional equivocation, and average information leakage rate.

2.3.3 | Alternative SOP

Although general SOP expression provides a fundamental characterization of achieving secure and reliable transmission, but unable to differentiate between reliability and security. So, the outage event mentions above can either imply a fault in achieving secrecy or that the receiver is unable to decode the transmitted message. An alternative SOP formulation is proposed by the authors in Reference 47, which directly measures the probability of the transmitted message failing to achieve perfect secrecy. In this, the rate difference $R_E \triangleq R_B - R_S$, reverts the security cost when the message is transmitted. R_B and R_S are the rates of the transmitted message and confidential data, respectively. For the transmitted message, the legitimate receiver perfectly decodes if $C_B > R_B$, whilst perfect secrecy fails if $C_E > R_E$. Here the authors define SOP as conditional probability conditioned upon the message actually being transmitted

$$SOP_A \triangleq P_r\{C_E > R_B - R_S | message\ transmission\} \tag{8}$$

Unlike, SOP this formulation provides explicit measures of the security levels, as it considers the rate of transmitted code as well as the condition under which the transmission has taken place. If the CSI of the Bob is known, this formulation gives flexibility to Alice to decide whether transmit or not. In this case, if Alice is transmitting, then transmission takes place at a variable rate depending upon the channel condition. In case of transmission at a constant rate, alternative SOP reduces to conditional probability. This parameter is revised in the literature,[48,49] due to its flexibility, it is considered as one of the promising performance metrics of the PLS system.

2.3.4 | Strictly positive secrecy capacity

The probability of SPSC is a fundamental benchmark in secure communication. It is the probability that the secrecy capacity C_s is always higher than 0. Mathematically it is given in Reference 8 as

$$P_{SPSC} = P_r(C_s(\gamma_B, \gamma_E) > 0) \tag{9}$$

This is guaranteed by keeping $R_s = 0$. In literatures 41,50-52, authors have analyzed security performance of the wireless system accounting on SPSC metric over various fading channels.

2.3.5 | Probability of non-zero secrecy

The PNZ allude to the occasions that the positive SC can be surely accomplished, namely $Pr(Cs > 0)$, thus representing its equation as given in Reference 53.

$$P_{NZ} = P_r(\gamma_B > \gamma_E) \tag{10}$$

2.3.6 | Average secrecy capacity

This metric provides the average confidential transmission rate. In the scenario where Eve is an active user and Alice has access to the CSI of Eve, ASC is considered as pivotal and primary performance metric. It is defined as the instantaneous SC averaged over γ_B and γ_E.This parameter is extensively explored in the literature.[54,55]

2.3.7 | Fractional equivocation-based metrics

Because of the limitations of SOP mentioned in the preceding section, authors in Reference 46 have proposed new fractional equivocation-based performance metric. Basically, fractional equivocation Δ, is a random quantity arising due to the fading characteristics of the wireless channel, and its distribution is obtained as per the distribution of the channel gains of the system. From Reference 46, we get the maximum attainable fractional equivocation for a given fading model of the wireless channel as

$$\Delta = \begin{cases} 1, & if\ C_E \leq C_B - R_s \\ ((C_B - C_E)/R), & if\ C_B - R < C_E < C_B \\ 0, & if\ C_B \leq C_E \end{cases} \tag{11}$$

Depending upon this following metrics are proposed in the literature

(i) Generalized SOP: This is applicable to the wireless system having a distinct level of security requirements which, is evaluated in terms of Eve's capability to decode the secret message. The generalized expression is given as

$$GSOP = P_r\{\Delta < \theta\} \tag{12}$$

where $0 < \theta < 1$ represents the minimum reasonable value of the fractional equivocation. Here Eve's skill to decrypt the confidential message is set by selecting different values of θ. For instance, the conventional SOP is a particular case of the GSOP for $\theta = 1$.

(ii) Asymptotic Lower Bound on Eve's Decoding Error Probability: This metric is defined as the average of the fractional equivocation and is given by $\overline{\Delta} = \mathbb{E}\{\Delta\}$ in which $\mathbb{E}\{.\}$ is the expectation operation. It is worthwhile to mention that, when the entropy of data for transmission is long enough, Eve's decoding error probability for a given fading condition is lower bounded by the fractional equivocation, that is, $P_e \geq \overline{\Delta}^2$.

(iii) Average Information Leakage Rate: This metric offers an idea of how fast the data is leaked to the Eve, when an unchanged rate transmission R_S, is adopted in the system. It can be expressed as

$$R_L = \mathbb{E}\{(1 - \Delta)R_S = (1 - \overline{\Delta})R_S \tag{13}$$

2.4 | PLS with finite-alphabet signaling

The review discussed so far considered a Gaussian distributed input. The detection complexity of the Gaussian signal is high as it takes continuum values, in addition to this the amplitude of the Gaussian signals is unbounded, so Gaussian signaling is not typically used in practice. However, practically, the transmitted signals are drawn from discrete signal constellations such as PSK and QAM. Hence, understanding the impact of the finite-alphabet input constraints and designing secure transmission schemes under this assumption is a mandatory step toward the practical implementation of PLS. In Reference 56, the authors evaluate the constellation-constrained SC, and highlight an important behavioral difference between finite-alphabet (eg, PSK and QAM) and Gaussian inputs, that is, for a fixed noise variance at Eve, the SR curves for PSK or QAM plotted against the SNR have global maxima at finite SNR values. Investigation of the SC of the PAM inputs over a degraded Gaussian wiretap channel in Reference 57, also leads to a similar conclusion. A comprehensive review of recent developments in PLS with finite-alphabet signaling is provided by the authors in Reference 58. Authors have also included the review for secure transmission with discrete signaling over various scenarios including multi-carrier transmission systems, broadcast channels with confidential messages, cognitive multiple access and

relay networks in context with the important behavioral differences of discrete vs Gaussian inputs in the context of the PLS. In Reference 59, authors investigate the secrecy performance of FDA systems exploiting finite-alphabet inputs over fluctuating two-ray fading channels by deriving closed-form expressions for average secrecy rate and SOP. Specifically, a squared M-ary QAM scheme is considered due to its extensive applications in practical systems. PLS performance of AN aided MIMO channel with finite inputs is studied in Reference 60. An energy-efficient PAM-constellation alignment to form a received sizeable PAM constellation by adaptively aligning the power of multi-user's PAM sub-constellations is designed, which provides a new finite-alphabet non-orthogonal multi-access scheme. In a secure spatial modulation communication with finite alphabet inputs, AAG selection methods are investigated in References 61,62 to enhance the SR. In former, an accurate approximation of the SR is used for reducing the computational complexity, and the optimal AN covariance matrix is found by convex optimization for any given AAG, when only rough partial CSI of Eve is obtained at the transmitter. The convex optimization is solved using fractional programming. Whereas in the latter, two antenna selection methods with low complexity, Max-SR I and Max-SR II are proposed which is enhanced by using AN. Using the SR expression, the problem of maximizing SR, called Max-SR I, is converted to an integer programming problem. In the high SNR region, an asymptotical lower bound for SR is derived to prove the fact that the Max-SR can be reduced to maximizing the difference of Bob's minimum Euclidean distance and Eve's one, called Max-SR II. The impact of transmitter-side correlation on the artificial-noise-aided secure transmission is studied in Reference 63. Specifically, a correlation-based power allocation for AN, of which the optimality in terms of achieving the minimum SOP is analytically proved in the large system regime with the number of transmit antennas approaching infinity.

3 | REVIEW OF RELATED SURVEYS AND MOTIVATION

A number of surveys related to PLS are available in the literature. In Reference 64, the technologies used in PLS and the related challenges and solutions are provided. More specifically, the major challenges associated with conditions of the channel along with the numerous solutions such as channel estimation technologies, coding and pre-coding techniques, signal processing, and so on, available in the literature are comprehensively explored in this paper. A survey of PLS researches over various technologies of the 5G network such as mm-wave communication network, heterogeneous network, NOMA, full-duplex network, and massive MIMO network is provided in Reference 65. Also, a review of the state-of-the-art of three significant PLS codes, including LDPC codes, polar codes, and lattice codes are presented. Authors in Reference 66 also provide a review over the PLS trend in 5G network. The difference between these two surveys is that the latter includes a comparative study of the various approaches of the PLS used in the 5G communication network. Also, presents a review of the PLS solution dedicated to major applications of the 5G communication, such as constellation-rotation-based signal design for upgraded secrecy in D2D communications, fine-grained security level portrayal, and measurable security ensure for services having delay constraints and fountain coding aided security improvement for IoT applications. A review of technical challenges in providing security in the physical layer for the 5G enabled network is explored by the authors in Reference 67. In Reference 68, the state-of-the-art of optimization and design research of fundamental optimization problems, that is, maximization of attainable secrecy rate, minimization of SOP, minimization of power consumption, and maximization of secure energy-efficiency strategies are investigated to provide deep insights into secure transmission designs. In Reference 69, authors have conducted a review of the works on securing the FSO and VLC systems using the PLS mechanisms, and a comparative study of RF communication systems with these systems is also done. Whereas in Reference 70, exclusive review over the MIMO, MISO, SISO, and hybrid VLC for single and multiple users is provided. The information-theoretic and signal processing techniques of PLS for the VLC system is revised along with the impact of different VLC features on the security performance. In a multiuser broadcast system, multiple accesses relay networks, and interference networks, approaches for the secrecy based on channel coding design for security improvement are reviewed in Reference 71. The state-of-the-art of PLS security in cooperative relay wireless network is reviewed in the literature.[72] Similarly, for the massive MIMO, passive and active attack in PLS system is reviewed in Reference 73. A comprehensive survey focusing on the classification and applications of the PLS technique on providing confidentiality of the system is explained by the authors in Reference 74. In this, explaining the basic physical model, authors have provided various security technique classifications in time, frequency, and space domain security. The diversity techniques for improving the PLS over the IoT is explored in literature.[75-77] In Reference 78, an extensive survey over the PLS investigating the existing security protocols, and algorithms are

TABLE 3 Existing surveys over PLS and contributions

Reference	Focused issue	Main contributions
64	Review of the fundamental theories, technologies and challenges of PLS	Studies the technologies, challenges, and solutions in PLS from the aspects of wiretap coding, MIMO, and relay cooperation, physical-layer key generation, and physical-layer authentication
65	Review of PLS techniques and challenges in 5G network	A comprehensive survey of the state-of-the-art of important PLS codes
66	PLS and its applications in 5G network	Provides a comparative study of various PLS approaches, and PLS solution for the 5G applications
67	PLS in safeguarding 5G network	Identifies the scientific opportunities and the technical challenges offered by the 5G enabled networks such as HetNet, massive MIMO, and mm-Wave communication for achieving PLS
68	Optimization approaches for wireless PLS	Reviews design research of fundamental optimization problems, such as maximization of obtainable secrecy rate, minimization of SOP, minimization of power consumption, and maximization of secure energy efficiency strategies
69	PLS over FSO communication	Presents a comparative review of PLS over RF communication and optical wireless communication
70	PLS over VLC	Reviews the PLS techniques for MIMO,SISO, MISO, and Hybrid VLC communication networks including both information-theoretic and signal processing aspects of the VLC system
71	PLS over the multiuser wireless network	Reviews security improvements in multi-antenna, broadcast, multiple-access, interference, and relay channels, as well as physical layer key generation and secure coding
72	PLS in relay cooperative networks	Presents a pure or hybrid relaying or jamming combination of secrecy improvement of the trusted or untrusted relay cooperative network
73	PLS for massive MIMO.	Discussing the passive eavesdropping and active attacks in massive MIMO systems while proposing three detection schemes to identify the active attacks
74	Survey on the application of PLS for confidentiality	Provides a comprehensive review over SINR-based methodology and complexity-based methodology for passive ED
75	Diversity techniques to improve PLS	Exploiting MIMO diversity, multiuser diversity, and cooperative diversity to secure wireless communications
76	PLS in the IoT	Surveys the advances and difficulties in resource-constrained secrecy coding and secret key generation in the IoT
77	Challenges and solutions of PLS for IoT	Reviews the problems with various approaches of the PLS in IoT applications and formulates the solution
78	Security vulnerabilities, security threats, and efficient defense mechanisms.	Discuss the security requirements and attacks at each protocol layer, investigating the existing security protocols and algorithms, while exploring the state-of-the-art in PLS

included by the authors. Table 3 highlights the summary of the existing surveys available and the main focused issues in the literature.

3.1 | Motivation

After exploring the literature, it is found that the vast majority of these overviews survey the PLS-based communication, channel types, or the propagation scenario, including the information-theoretic approach. The literature still lacks in the review of the PLS measures on the various wireless fading channels, motivated by this gap, this paper highlights

the survey of the PLS over the fading channels, which has not been explored in the literature yet. As explained, PLS utilizes randomness of the wireless channel to provide security, this randomness is modeled by various fading models. So it is essential to study the PLS over the fading models to gain insights into the communication system. This work distinguishes itself from the existing surveys in these respects. Most of the surveys[71-73,75] presented are scenario dependent such as multiuser, multi-antenna, and cooperative communication. Even though they provide a comprehensive and structured review of PLS over these scenarios but unfortunately lack in explaining the generic concept of keyless approach of PLS and the performance metric. The organization of this survey differs from Reference 74, rather than going through the complexity-based and SINR-based approach, this paper provides a comprehensive review of the various analytical expressions for the performance metrics of PLS in terms of their complexity which has not been included in any of the published surveys. A clear classification of PLS based on the type of ED is thoroughly reviewed in this paper, however, few of the existing surveys such as References 64-66 have focused on the state-of-the-art and the PLS techniques but lack the review of some recently published survey. Additionally, this review exclusively focuses on the application of the PLS concept over the several wireless fading channels, which has not been included in the existing surveys. Comparing with the surveys previously presented, this survey paper aims to provide in-depth technical discussions about the optimization approaches adopted in the literatures to enhance the PLS of the system. Also, it includes the review of contributions made to ensure PLS with the finite input signaling which has not been well explored in the existing surveys. To facilitate and inspire research in the analysis, design optimization, and implementation of the network ensuring security at the physical layer, a comprehensive discussion over all the aspects of the PLS design is presented in this survey paper. Moreover, a descriptive review of the PLS in emerging wireless communication such as IoT, D2D, V2V, BAN, VLC, and UAV communication is also presented as well as new future directions of application of PLS in IRS system is thoroughly discussed.

4 | PLS CLASSIFICATIONS

In this section, we provide a comprehensive survey of the PLS based on the various fading models, type of ED intruding the communication link and PLS on the emerging wireless communication applications. In the fading model-based survey literature available on the multipath, shadowing, and composite fading models[79-81] are investigated whereas in ED-based classification active and passive ED is thoroughly explored. Implementation of PLS over various wireless communication applications such as V2V, IoT, UAV, BAN, and so on, is also studied. The schematic classification of the PLS work performed in this work is depicted in Figure 6.

4.1 | Based on fading models

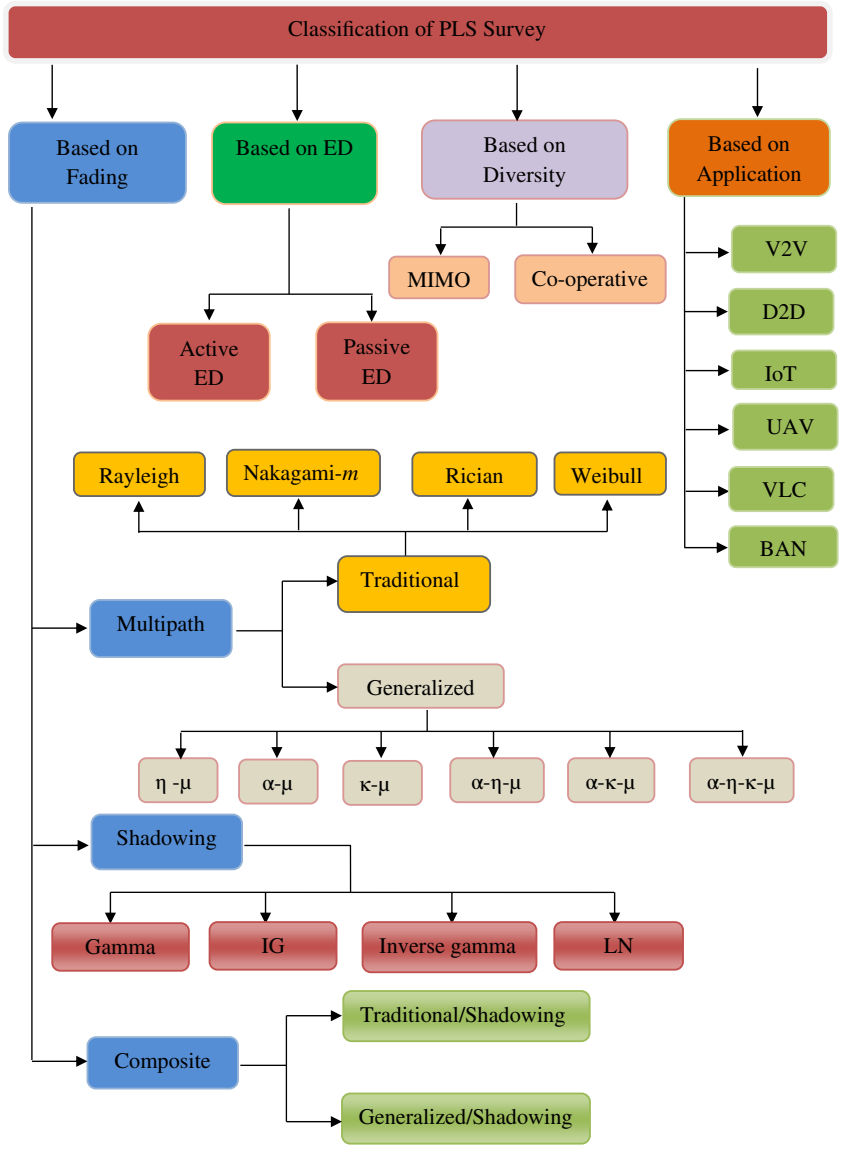
This section, presents a comprehensive survey over the literature available to analyze the performance of PLS over various multipath, shadowing, and composite fading models. These models are extensively used to characterize the random nature of the wireless propagation medium. In the PLS, this intrinsic characteristic of the channel is utilized to provide security.

4.1.1 | Multipath fading model

Due to the channel impairments when multiple superimposed copies of the same signal reach the receiver this tends to degrade the signal, this degradation of the signal is termed as multipath fading. The multipath fading is divided into two categories, traditional and generalized. Below is the description of each fading model.

(i)Traditional fading model: It describes the basic fading distributions such as Rayleigh, Nakagami, Rician, Weibull to model the multipath fading.[82] Rayleigh fading is more prominent when there is no line of sight communication between the transmitter and receiver. In Reference 83, SC analysis over the joint PDF of correlated Rayleigh fading wiretap channel is done, proving that if the average CGR is higher than power correlation co-efficient, SC remains unaffected from correlation. In Reference 41, an analytical expression for the SC and SOP over Rayleigh faded main and ED channel in the form of infinite series is derived whereas in Reference 84, the recursive process is used to estimate the SC. To

FIGURE 6 Classification of PLS survey



estimate the channel characteristics using infinite series is a complex process, so in Reference 85 a closed-form expression for the SC and SOP over the correlated Rayleigh fading in terms of widely used Marcum Q function is provided. In Reference 23, the achievable SR for the system where the main channel being the AWGN channel and the ED's channel undergoing Rayleigh fading is analyzed. It is shown that even if the main channel gain is arbitrarily worse than the ED's average channel gain, using burst signaling and artificial noise injection techniques, positive secrecy rate can still be accomplished. For applications such as V2V communication where the location of the ED is uncertain and the channel is Rayleigh faded, SC analysis is provided in References 54,86. With full CSI or only with the CSI of the legitimate user, SC over the Rayleigh fading channel is investigated in Reference 87. After Rayleigh fading, Nakagami-*m* is the extensively used fading model. SC analysis over Nakagami-*m* fading channel in the presence of multiple, and co-operative ED is done in References 42,88. From the results presented in the paper, it is observed that raise in the number of EDs degrades the SC. Also, the correlation degree between the EDs has a negative impact on the SC of the channel. In Reference 89, secrecy analysis with diversity in the wiretap channel experiencing Nakagami-*m* fading is done, concluding with the fact that the diversity order of the main link must be increased to achieve the high secrecy requirement.

An integral formula for SOP incorporating different transmission factors, including node density, correlation coefficient, and fading parameter, is derived in Reference 90. The findings of the paper show that the impact of channel correlation is selective, that is, enhances secrecy rate when secrecy outage is more significant than 50%, and degrades

when secrecy outage is less than 50%. Considering the main channel undergoing Rayleigh fading and wiretap channel experiencing Nakagami-*m* fading, exact closed-form expressions for SC and SOP of the SISO system is derived in Reference 91. In Reference 92, authors have derived an expression for the achievable secrecy rate under the different assumption of transmitter CSI for the Nakagami-*m* MISO system, proving that multiple antenna transmit systems can improve the SR. A closed-form expression for ASC, SPSC, and SOP in terms of bivariate and univariate Meijer's G function over the cascaded Nakagami-*m* fading channel is derived in Reference 93. A reliable approach to evaluate the secrecy performance of the underlay cognitive radio system over the Nakagami-*m* fading channel is provided in Reference 94.

Unlike Rayleigh fading, Rician fading model has at least one dominant line-of-sight component, out of several different received signals. In Reference 95, a novel and exact expressions for the SOP and PNZ for the PLS over the double shadowed Rician fading channels is derived to evaluate the PLS performance. In the analysis it has been shown that the multiplicative shadowing parameter has a larger impact on the SOP than the line-of-sight shadowing parameter. Analysis of probability of SPSC of the system in which main channel and ED channel suffering from Rician fading is done in Reference 52 and for legitimate channel and ED channel suffering from Rayleigh/Rician and Rician/Rayleigh fading, respectively is provided in Reference 96. This fading model is used in wireless communication with its implementation in an indoor and outdoor environment. The impact of various fading parameters on the SPSC of the Weibull faded legitimate, and ED channel is analyzed in Reference 50. With CSI available at the legitimate transmitter first considering single ED and then double ED, ASC over the Weibull fading channel is done in Reference 55.

(ii).Generalized Fading models: Generalized fading[97-100] models such as α-μ, κ-μ, α-κ-μ, and η-μ provide a general framework to model fading with the combination of various practical fading models. Because of its versatility to accommodate the practical fading model, it is termed as generalized. Secrecy analysis over the α-μ fading channel is widely explored in the literatures. An analytical expression for the probability of positive secrecy capacity and upper bounds of SOP is derived in Reference 101. As the expression derived in Reference 101 is in terms of hypergeometric function which is complex to solve, so in Reference 40 closed-form expression in the terms of well-known Meijer G function is derived. The physical analysis of the expression concludes that for the fixed value of the power of the wiretap channel, the probability of positive secrecy capacity is high for the higher power of the main channel. Secrecy analysis for point to point communication over the α-μ fading channel is provided in References 102-104. A closed-form expression for the ASC in terms of EGBFHF is derived in Reference 102. Asymptotic analysis of SOP expression in the terms of bivariate Fox H function for the SIMO α-μ fading and considering randomly distributed EDs is done in References 103,104 respectively.

Authors in Reference 105 have considered an α-μ faded MIMO wireless network, where both the locations of legitimate receivers and EDs are modeled with two independent HPPPs. Then the secrecy metric analysis is done with respect to the *k-th* nearest or best user, as the best user represents large and small scale fading compared to the nearest one, it gives the overall impact when estimating the secrecy performance. In terms of security analysis, the SOP and the PNZ for the cascaded α-μ fading channel in the presence of active ED is analyzed in Reference 106, and closed-form expressions are derived in terms of the Fox H function. The performance analysis of PLS over another generalized κ-μ fading channel is done in Reference 107. In this paper, authors have derived a closed-form expression of SPSC and SOP for the κ-μ fading channel considering the positive, real and n.i.n.d channel co-efficient. To prove the versatility of the derived equations Rayleigh/Rayleigh, Nakagami-*m*/Rice and other fading channels as a special case is studied. To demonstrate the efficacy of the derived expressions, the probability of SPSC of real-time applications such as D2D, V2V, and body-centric fading channels based on the field measurements is provided. In Reference 108, analytical expressions for the SOP in a SISO system over κ-μ fading are derived, whereas Reference 109 derives the SOP and ASC expression in a SIMO system undergoing κ-μ fading considering full CSI in both the cases. In Reference 45, authors have considered two types of channel conditions. In the first condition, main channel and wiretap channel are experiencing α-μ and κ-μ fading respectively whereas in the second condition wiretap channel is α-μ faded while main channel is κ-μ faded. A novel expression for the SPSC and SOP^L in terms of well-known Meijer G function is derived and the behavior of SOP and SPSC is also studied for various fading parameters.

The α-κ-μ and α-η-μ distribution is used by the authors in Reference 110 which comes out to be a more generalized fading model as compared to the previous ones, as it accommodates the characteristics of all other traditional models as a special case. In Reference 44, a closed-form expression of the SOP^L for the α-κ-μ and α-η-μ fading channel in terms of Fox H function is derived along with the asymptotic analysis of SOP. To analyze the performance of PLS over α-η-κ-μ fading channel, which is considered as the ultimate generalized model,[111] an expression for ASC in terms of EGBFHF, and SOP

in terms of the Meijer G function is derived in Reference 112. In this, authors have also presented the comparison of ASC for various fading channel considering as special cases of α-η-κ-μ. The B-X fading distribution[113] is composed of multiple numbers of LOS components with some diffused power, PLS performance over B-X faded main and wiretap channel is explained in Reference 114.

Analytical expressions of ASC, SOP, and SPSC for the B-X channel are derived and the impact of various fading parameters on these metrics is studied. Furthermore, the asymptotic analysis of ASC under high and low SNR regime is also conducted. A closed-form expression for the SOP^L is also derived.

4.1.2 | Shadowing models

In wireless communication systems, the communication channel is additionally influenced by the slow variation of the mean signal level because of shadowing from the terrain, building structures, and trees. To model this variation, LN shadowing model[115] is extensively used. The mean and distributions of path loss signals that are treated as an arbitrary variable are used to model the characteristics of the channel. PLS analysis of the wireless channel subjected to LN fading is investigated in Reference 116. Here, the authors have derived an expression for SPSC considering two conditions of a wireless system, first the main channel along with single ED and second with two EDs undergoing LN fading. The expressions are deduced in terms of the Gaussian Q function. From the findings, it is also observed that the SPSC decreases significantly because of the presence of the second ED. Similarly, in Reference 117, closed-form expressions of the probability of SPSC for wireless communication systems, with two and three EDs, respectively experiencing lognormal fading is derived. These expressions are in terms of the well-known T-function and S-function. In Reference 118, the analysis focuses on the OP of secrecy capacity for a system in which the main channel and the ED channel are subject to the correlated LN fading. It is also shown that correlation improves the performance of the system with regard to the outage probability. Employing diversity combining techniques, MRC, and EGC reception at the legitimate receiver and ED, a closed-form expression for the secrecy parameters is derived in Reference 119. It is concluded in the paper that diversity enhances the security of the channel and the effect of diversity increases with an increase in shadowing parameter at the main channel and ED channel.

4.1.3 | Composite fading models

Composite fading models[120-125] are best suitable to describe the statistical behavior of the real-time propagation channel which experiences shadowing and multipath fading simultaneously. The abundance of literature is available to account for the performance of PLS over the composite fading channels. For example, performance of PLS metrics over the κ-μ shadowed channel is investigated in the literatures.[126-128] The ASC and SOP analysis for the integer fading parameter using incomplete moment generating function framework is done in Reference 129, and the expression is derived in terms of bivariate confluent hypergeometric function. Similarly, lower bounds on SOP and SPSC using the PDF approach are derived in Reference 126 over the κ-μ shadowed channel. However, the results in these papers are presented in terms of double infinite series, which is not feasible for further computation, so in Reference 127, using the method of moment matching novel representations of the lower bound on SPSC and SOP are deduced over independent κ-μ shadowed model. To deal with the infinite series problem, the moment matching method is used. While Reference 128, provides SPSC and SOP analysis in the terms of Gauss hypergeometric function. In Reference 130, analytical expression in the terms of Meijer G function for the SOP and PNZ over the correlated Nakagami-*m*/gamma composite fading channel is derived. On the basis of numerical analysis, it is shown that SOP degrades because of the severe correlated shadowing in the receiver and ED, even if multipath fading is between these nodes is independent. Secrecy analysis over the SISO generalized K and SIMO generalized K channel is provided in References 43,131, respectively, which is basically a composite of Nakagami-*m*/gamma distribution. The expressions for the performance metric are derived in terms of EBGMGF. However, only lower bound analysis for the SOP is provided because of the complexity of the expression. Secrecy analysis over F-S composite fading channel under the various shadowing conditions is studied in References 132,133 over the same channel closed-form expression for the SOP and ASC in terms of Meijer G function is derived considering a special case of D2D communication. Over the Weibull/lognormal[134] composite fading channel, PLS performance metrics are evaluated in Reference 135.

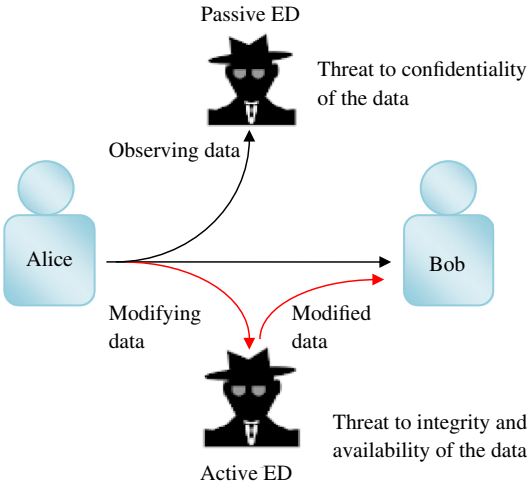


FIGURE 7 Passive and active ED scenarios

4.2 | Based on the type of ED

To design an effective eavesdropping scheme, it is important to be aware of the behavior of the ED. Specifically, EDs are of two types, passive and active. The major difference between them is that active ED has the potential to intercept the connection and modify the message being transmitted between Alice and Bob. In contrast, passive ED only listens to the information being transmitted and does not have the intention to modify it. Figure 7 shows the functionality of passive and active ED affecting the communication links, respectively. In active eavesdropping, the attacked entity is aware of the attack, but in passive eavesdropping, it is unaware of the attack. Since passive ED does not expose itself, their study is much more challenging than the active ED. In this section, review of the fading channel undergoing active and passive eavesdropping is presented.

4.2.1 | Passive ED scenario

Passive ED scenario applies to the wireless communication networks where Eve is silent, so the corresponding CSI is not known to Alice. In this scenario, SOP is the best suitable secrecy performance parameter to analyze the channel. In Reference 136, a closed-form expression for the SOP^L and asymptotic analysis at high SNR over the α-η-μ and α-κ-μ fading channel is done where a passive ED attempts to intercept the information transmitted on the legitimate link. The impact of fading parameters and ED SNR is analyzed, showing that for incremental values of ED SNR, SOP degrades regardless of the SNR at the main channel. For the same system model, secrecy analysis of Nakagami-*m* fading channel with multiple and cooperative EDs is done in References 42,88, respectively. The results conclude that with the increase in the number of ED, SC decreases. The SOP over α-μfading channels was studied in Reference 40, and the expressions for the SOP bound, and the SPSC is derived considering the passive ED. Similarly, for Malaga-Malaga fading channel, an exact integral expression for SOP is deduced in Reference 137. Since the integral expression is hard to use in analysis, a closed-form expression for lower bounds of SOP is derived in terms of the Meijer G function. In Reference 5, authors have derived a closed-form expression of SPSC, and SOP for the κ-μ fading channel considering the positive, real and i.n.i.d channel co-efficient. To prove the versatility of the derived equations Rayleigh/Rayleigh, Nakagami-*m*/Rician, and other fading channels as the special case have been studied.

To demonstrate the efficacy of the derived expressions, the probability of SPSC of real-time applications such as D2D, V2V, and body-centric fading channels based on the field measurements is provided. Authors in Reference 107, focus on the SOP analysis of SC for a communication system where the main channel and the ED channel are subjected to the correlated LN fading. It has been shown that correlation improves the performance of the system with regard to the OP. For the independent LN fading channel with passive ED, an analysis of SOP and PNZ is provided in Reference 51. For the M-distributed fading channel, an exact expression of SOP is derived in Reference 138 considering passive ED. This paper also provides an analysis of secure performance of the generalized K, gamma-gamma, and exponential fading channels as the special case of M -distributed fading channel.

4.2.2 | Active ED scenario

When the perfect CSI of the legitimate user and the ED is available to the transmitter, then this condition is called active eavesdropping. In the scenario of active eavesdropping, the malicious node actively grabs the information transmitted over the main channel by sending queries to the transmitter and disguising themselves as a friendly node. ASC is the best-suited performance metric to analyze the PLS in this scenario. Many researchers have focused on this parameter to analyze the secure communication. In Reference 84, a system model with active ED is considered for the analysis of secrecy analysis over co-related Rayleigh fading. The expression for ASC is derived in integral terms, which is complicated, so a simple expression in terms of the Marcum Q function is provided in Reference 85 over the same channel. In Reference 83, the expression for the SC using the joint PDF of the correlated Rayleigh fading wiretap channel is derived. Also, from the asymptotic analysis, it is concluded that SC depends on the two channel parameters: average CGR and PCC. Furthermore, after analysis, it is shown that, the correlation does not affect the secrecy capacity when CGR is high. In Reference 131, analytical expressions for ASC of SIMO systems are derived via two different methods, in which using Gamma and MoG distribution generalized-K fading is approximated. Authors have characterized the SC of the slow-fading channel in Reference 17 with an ED under various suppositions on the available transmitter CSI. This work sets up an intriguing outcome that a non-zero perfectly secure rate is attainable in the fading channel even when the ED is more competent than the legitimate receiver. Also, it proves that the knowledge of the main channel CSI, however, is crucial since the absence of this information prompts a zero SC when the ED is more proficient than the genuine receiver. The SC of an ergodic fading wiretap channel, when the main and ED channels are correlated and assuming that the transmitter knows the full CSI, is studied in Reference 23. The secrecy capacity using the joint PDF of the correlated Rayleigh fading wiretap channel is derived, which converges to a finite value as SNR reaches infinity. Asymptotic ASC is also derived in terms of two parameters average CGR and PCC. For the arbitrarily varying wiretap channel, strong secrecy criterion is studied in Reference 139. Authors have derived a lower bound expression on the random code secrecy and an upper bound for the deterministic code secrecy, which explicitly provides SC expression in special cases. In Reference 140, authors analyze the arbitrarily varying wiretap channel experiencing jamming attacks and study the analytical properties of both deterministic and common randomness-assisted secrecy capacities. A brief summary of the above work is given in Tables 4 and 5 respectively.

4.3 | Based on diversity

This section concentrates on the review of the diversity-based PLS security approach that is being used in literature such MIMO diversity and co-operative diversity techniques. Diversity basically refers to a method for improving the reliability of the message signal by using two or more communication channels with different characteristics. This technique is also used to enhance the PLS of the wireless communication systems.[142] Table 6 provides the techniques and contributions of the work based on the application of diversity on PLS.

TABLE 4 PLS over fading channels with passive ED

Reference	Fading channel	Contributions
136	α-η-μ and α-κ-μ	SOP^L and asymptotic SOP analysis
88	Nakagami-m with cooperative ED	SOP analysis
25	Nakagami-m with multiple ED	SOP, PNZ and outage secrecy capacity analysis
40	α-μ(GG) fading channel	Lower bound SOP and SPSC analysis
137	Malaga-Malaga fading channel	SOP analysis
141	Co-related lognormal fading channel	SOP analysis
51	Independent LN	SOP, PNZ analysis
138	M-distributed fading channel	SOP analysis

TABLE 5 PLS over wireless fading channels with active ED

Reference	Fading channel	Contributions
83-85	Co-related Rayleigh fading channel	ASC and ESC analysis
15	Independent Rayleigh fading	ASC analysis
133	F-S composite fading channel	ASC analysis
53	Fox's H wiretap channel	ASC analysis
59	N-Nakagami fading channel	ASC analysis for the mobile vehicular network
131	SIMO generalized K fading	ASC analysis using gamma-based method and MoG-based method
17	Ergodic fading channel	Perfect SC analysis along with the optimal power and rate allocation strategies
23	Co-related ergodic fading channel	ASC analysis

TABLE 6 Survey on diversity-based PLS techniques

Reference	PLS technique	Contributions
143	MIMO diversity	Explains beamforming schemes for MIMO wiretap channel to ensure PLS
90	MIMO diversity	SOP analysis over κ-μ and η-μ wiretap channel implementing MRC at the receiving end
105	MIMO diversity	SC analysis over MIMO, α-μ fading channel
22	Co-operative diversity	Secure communication over co-operative relays
144	Co-operative diversity	Implementation of co-operative jamming to provide PLS
145	Co-operative diversity	Analysis of secrecy gain for a network with untrusted relay

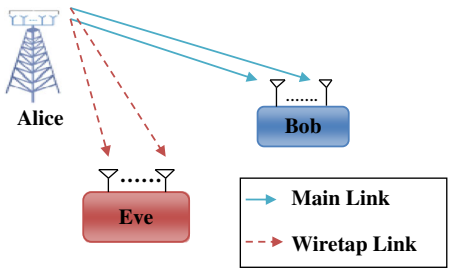


FIGURE 8 MIMO wireless system with ED attack

4.3.1 | MIMO diversity

The MIMO diversity is widely applicable to the various cellular and Wi-Fi applications, whereas co-operative diversity is applicable to some specific advanced Wi-Fi or cellular applications such as LTE advanced system where relaying is introduced to assist wireless transmission. Figure 8 shows the typical MIMO wireless network in which the legitimate transmitter with multiple antennas is communicating with the legitimate receiver having multiple antennas in the presence of ED. In Reference 143, a powerful beamforming technique that recovers a large fraction of the performance in the perfect CSI case for a MIMO wiretap channel is discussed by the authors. In Reference 146, a seminal work over the heterogeneous network which adopts MRC[147] to achieve the secure transmission is presented. In Reference 105, PLS over the MIMO, α-μ channel is well explained whereas in Reference 71 various diversity combining techniques have been implemented at the ED and legitimate receiver end to enhance the secure reception.

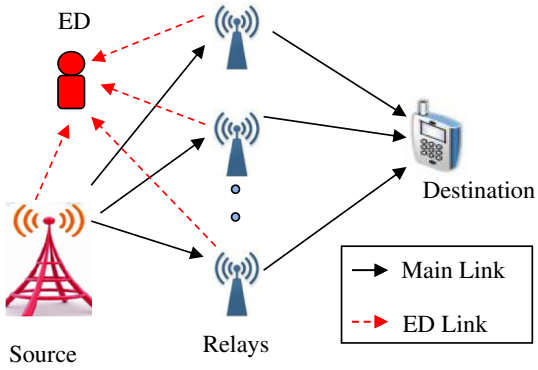


FIGURE 9 Co-operative diversity system consisting of source, destination and ED

4.3.2 | Co-operative diversity

In co-operative communication, the communication between two nodes takes place via a relay that is located between the source and the destination nodes. Besides providing reliability and high coverage, this concept is also extended to the PLS of the system.[142] A generalized co-operative diversity network with ED is given in Figure 9. In Reference 22, authors have introduced secure communication over the cooperative relays. Authors have considered three co-operative schemes that are, DF, AF, and cooperative jamming and proposed system designs subjected to transmit power constraint. Using co-operative jamming to provide PLS in wireless wiretap channels via distributed relays is studied in Reference 144. In Reference 145, authors have presented the study of achievable secrecy gain of the co-operative networks with untrusted relays, showing that with a decrease in the number of the untrusted relays, SR increases.

4.4 | Based on application involving PLS measures

As mentioned emerging next-generation wireless network supports a wide range of complex, diverse applications. These applications demand immense capacity of data and put forward for the high data security demand. Many researchers have taken an effort to investigate the special characteristics and requirements of these high demand emerging applications. Under this line, PLS has become an important measure to account for. To illustrate the in-depth understanding of the PLS measures and how it affects the performance of the system over different application scenarios, various case studies have been investigated in the literature. This section provides a comprehensive review of applications such as D2D, V2V, UAV, BAN, VLC, and IoT communication.

4.4.1 | D2D communication

D2D communication allows the user equipment placed in close proximity to communicate using direct link rather than their radio signal traveling through AP. Due to the shorter signal traversal path, this provides an ultra-low latency in communication. D2D paradigm provides relatively high security in the physical layer, by reducing the exposure of the information from two relatively high power transmissions to a single low power hop. D2D communication scenario with ED is shown in Figure 10.

The red line represents the standard centralized cellular network communication, where device 1 first transmits the signal to the AP and then communicated with device 2 in second hops. The ED potentially wiretap the signal in both uplink and downlink communication. The solid black line represents the direct D2D communication link, ED can wiretap only this single-hop link, which is likely to be at low power to avoid interference from the other devices in the proximity. A comparative study of the PLS over the D2D communication link and the conventional cellular link is comprehensively provided in Reference 148. The expression for the SOP for both the cases considering statistical CSI information of the ED is derived. The analysis concludes that D2D model outperforms the cellular link in terms of providing security. More likely D2D pair maximizes their achievable data rates by reusing cellular user's resources without violating the secrecy requirement of the cellular user. Regarding improvement in the network security from the physical layer, there have been several works demonstrating that by acquainting underlaid D2D pairs to act as friendly jammers, the secrecy performance

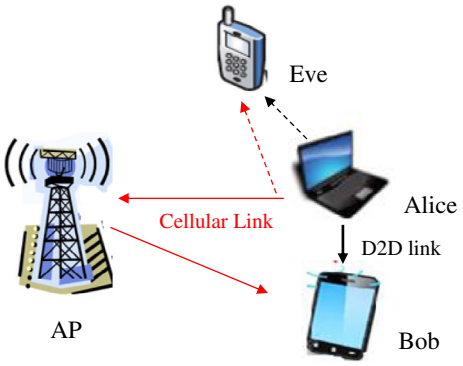


FIGURE 10 General model of D2D communication with ED

of a cellular system can be prominently enhanced. An explicit analysis over SOP is provided in Reference 149 for the secrecy-based access control in the D2D communication underlaying mobile network. Also, an expression for the optimal transmission power and access control mechanism is derived. In Reference 150, the authors used a weighted bipartite chart to formulate the coordinated matching issue between cellular users and D2D pairs regarding the secrecy concern of mobile users. In Reference 151, authors have derived the optimal joint power control solutions of both the cellular communication links and D2D pairs in terms of the cellular SC and secrecy-based control JPAC scheme with ideal D2D pair choice mechanism to accomplish improved system secrecy performance with less complexity. Authors in Reference 152 provide transmission secrecy of D2D underlaid cellular network and prove analytically that the sum secrecy rate of cellular users can be significantly increased by introducing D2D communication.

4.4.2 | IoT-based communication

IoT system allows the physical objects to sense communicate and perform certain actions on demand, supporting multitudes of applications such as smart cities, medical facilities, industrial monitoring, and so on. Figure 11 shows the various IoT-based applications. With a huge number of devices connected in IoT, wireless communication is a preferable medium to communicate. As discussed earlier, wireless communication is vulnerable to eavesdropping. Thus, there is a clear need to ensure the security of data on the fly to maintain secrecy. To guarantee security, the conventional approach is through the upper layer cryptographic algorithms and protocols. Besides, PLS utilizes the channel abnormalities to enhance security. In Reference 153 authors have discussed various PLS techniques such as artificial noise injection, compressive sensing, bit flipping, cooperative secrecy, and physical layer encryption used in IoT applications. To ensure secure communication, Reference 154 proposes an antenna design method based on ML, which can accomplish directional communication from the relay tag to the receiving reader by linking patch antenna with antenna LPDA for IoT. In Reference 155, study the secure uplink transmission scenario in IoT, where one of the multiple sensors communicate with the controller aided by the cooperative relay. An energy-efficient transmission scheme is proposed, which can be suitable for battery-limited devices and applications in IoT communication. Physical layer key generation and physical layer encryption security techniques are introduced by the authors in Reference 156, discussing their features, and applications by special consideration of IoT devices, low power, and low-cost features. Besides these, some more work dedicated to PLS security in the IoT system can be found in the literature.[157,158]

4.4.3 | VLC

It is emerging as a promising solution to the prerequisites of 5G, and beyond network, owing to the large unexploited spectrum. VLC systems are more immune against interference and more unsusceptible to security weaknesses since light does not penetrate through walls, security issues emerge normally in the VLC channels because of their open and broadcasting nature. These security issues needed to be carefully addressed and resolved in the VLC context. Extending the PLS security techniques to the VLC system is of great interest.

A typical VLC network consisting of the ED is presented in Figure 12. In this system, Alice employs a LED as a lighting source and at the receiver both, Bob and Eve are employed with the photodiode to detect the transmitted signal. When the

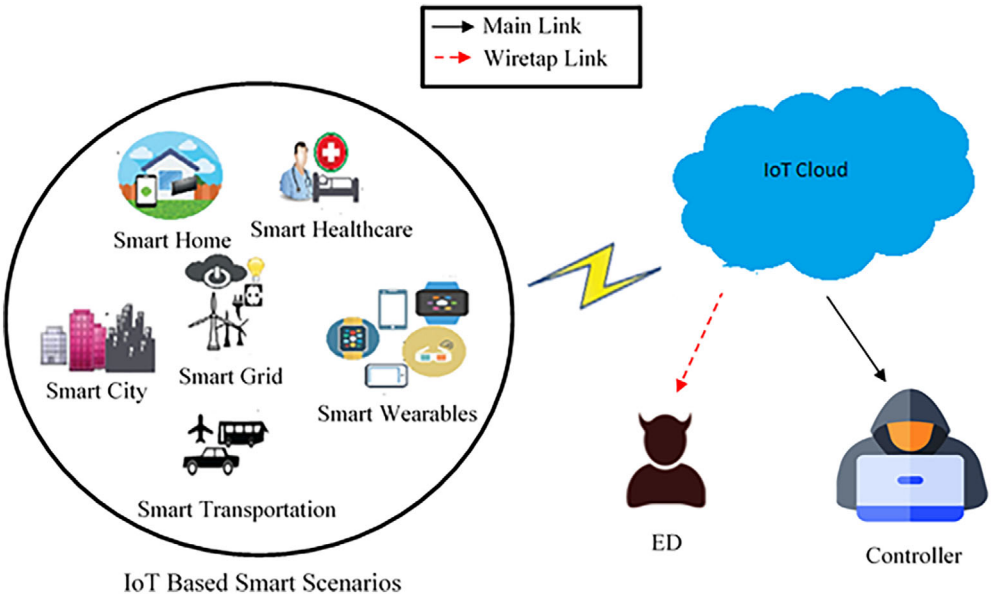


FIGURE 11 Visualization of an IoT wireless network with ED

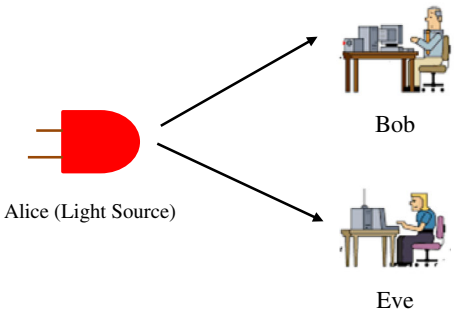


FIGURE 12 Typical VLC network with ED

active LED transmits the signal to the legitimate receiver, the ED also receives the signal as it also in the visible range of the light. Authors in Reference 70, provide a detailed review of PLS techniques available over VLC and RF communication. In this authors have considered the information-theoretic as well as signal processing aspect of VLC for SISO, MIMO, SIMO and hybrid RF/VLC system. For the indoor VLC system undergoing spatial modulation, a closed-form expression for the upper and lower bounds of the secrecy rate is derived in Reference 159. In Reference 160, authors investigate the SOP and SOP^{L} in an indoor VLC SWIPT system with randomly positioned receivers. In Reference 161, the influence of multiple reflections on the SOP of the VLC system for randomly distributed ED is studied. Considering a similar system, an expression for SOP as a function of the density of ED and geometric factors is derived in closed-form in Reference 162. The SC for the SISO, and SOP for multiuser VLC system is analyzed in the literature,[163,164] respectively.

4.4.4 | UAV communication

Due to the characteristics of agility, versatility, low cost, and easy-to-deploy, UAVs[165] are playing an important role in various areas. However, these benefits make UAVs more vulnerable to the ED attack as the information signals are transmitted over wireless channels.[166] Hence, security plays a significant role to isolate the information from the malicious ED attack. As UAV has limited resources specifically in terms of battery storage, a cumbersome cryptographic security approach is not much feasible. PLS has come up with an efficient measure to safeguard the wireless transmission from eavesdropping. Figure 13 shows a typical scenario of eavesdropping in UAV communication. In a UAV-based communication system, UAV may be a transmitter or receiver. When UAV is a legitimate transmitter, the air-to-ground LOS channel facilitates the signal reception both at the legitimate receiver and the ED. The passive ED tends to intercept confidential information without degrading the signal quality, whereas active ED intends to attack the information by some means such as using

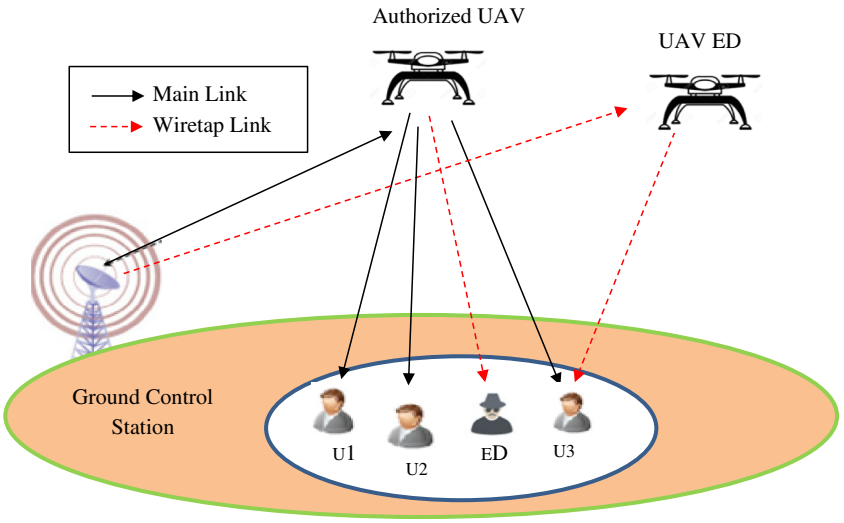


FIGURE 13 The general scenario of UAV communication links with eavesdropping

jamming signals. Various PLS techniques have been explored in the literature to ensure a secure transmission over UAV communication.

In Reference 167, comprehensive explanations on the challenges and opportunities in ensuring the PLS for UAV-based communication systems is provided. To improve the secrecy, UAV friendly jamming power is used in Reference 168, and expressions for intercept probability of the eavesdropper and the outage probability for the legitimate receiver is derived. Secrecy analysis over spatially random UAV is analyzed in Reference 169. A closed-form SOP expression for the air-to-ground and air-to-air link is derived considering the ED to be randomly distributed. In Reference 170, the closed-form approximation of the intercept probability and the ergodic SR for a UAV-assisted relaying system with single ED in urban environments is derived. The secrecy performance of the ground link in the presence of randomly deployed non-colluding unmanned EDs is investigated in Reference 171. The performance of secure connection probability with respect to transmitting-to-jamming power ratio, the height of the UAVs, and the UAV jammer location is also investigated.

4.4.5 | V2V communication

Vehicle-to-vehicle communication has drawn immense attention in recent years as it fuels to facilitate many future automotive applications such as safety services on highways, autonomous driving, roadway information dissemination, and infotainment services.[172] It allows vehicles or adjacent infrastructures to communicate with other vehicles, such as APs, or fixed equipment beside the road referred to as roadside units. To achieve security and privacy in V2V functionality, researches on PLS have attempted to create secure information communication strategies based on the physical attributes of the wireless channel.

The relationship between SC and the speed of a vehicle in the vehicular network is studied in Reference 173, concluding that a high speed of the vehicle may reduce SC. Also, a PLS technique using compressive sensing encryption is analyzed. The impact of the various vehicle, antenna, and noise-related parameter on the SC of the V2V communication system is studied by the authors in Reference 174. A comprehensive overview of the applicability of PLS in the area of vehicle-to-everything, including V2V is provided in Reference 175. The discussion has identified challenges and hurdles that need to be addressed to establish viable PLS protocols for establishing secure communication over such a system. A closed-form expression for the SOP and ESC for the cooperative vehicular system having a fixed source, destination node, and AF vehicle with passive ED is derived in Reference 176. Apart from these, some more work on PLS in V2V communication can be revised from the literature.[177,178]

4.4.6 | BAN communication

BAN communication is basically communication with implantable medical devices such as a cardiac pacemaker, neuron simulator, and so on. BAN comprises of actuators, and monitoring sensors that are small-sized smart units consuming

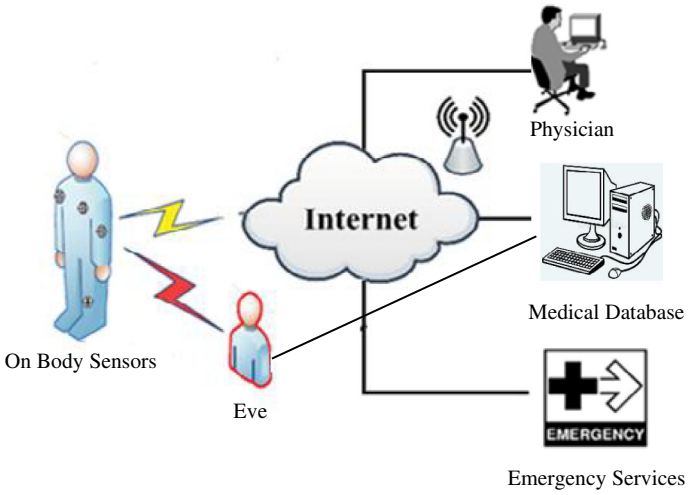


FIGURE 14 General BAN communication network with ED

ultra-low-power that are put at different explicit location inside and on the body and thus enables us to consistently examine and treat distinctive health issues.[179] The wireless technology makes BAN weaker toward various security threats such as eavesdropping or jamming, which could lead to serious issues. A general model of eavesdropping in the BAN network is given in Figure 14.

Security of the BAN network is a challenging issue as devices used in these are resource-limited, hence the PLS approach is considered as the most suitable approach because its features as discussed. Various PLS-based security approaches are discussed in several literatures. In Reference 180, the authors have analyzed the utilization of multi-hop relaying for the enhancement of PLS in the BAN. A comparative analysis of SOP for multi-hop and single-hop is also done, proving that multi-hop outruns the single-hop's SOP because of severe path loss in the human body. In Reference 181, authors presented a lightweight and simple encryption augmenting compressed sensing technique that provides security during the process of sampling an analog signal in a BAN. In Reference 182, a multi-hop topology utilizing game-theoretic Nash solution to optimize the SOP in an uplink wireless BAN considering the delay constraints is modeled. In Reference 183, a friendly jamming technique is proposed to protect the transmission against eavesdropping. This technique empowers the legitimate receiver to retrieve the transmitted signal effectively while the ED is kept shielded from decoding the transmitted signal. The main issue with this strategy is that it cannot work within the sight of malicious jammers. In Reference 184, a security method to make sure about information provenance for body-worn devices utilizing spatial and temporal characteristics of the wireless channel are proposed. The solution empowers the authorized users to produce correlated fingerprints and associate a data session uniquely with a wireless link, which are difficult for an ED to forge. Using experiments, authors have validated this technique and optimized the results in concern to resource constraints.

5 | OPTIMIZATION OF PLS-ASSISTED WIRELESS NETWORKS

5.1 | Theory of optimization

Secure strategies design based on the technique of optimization and signal processing is one of the major aspects of the studies related to PLS. To better understand the concept of optimization, let us take the general optimization problem formulated in Reference 185 as

$$\min_{x} f(x) \;\; such\ that \;\; \left\{ \begin{array}{l} h_i(x) \leq b_i, i = 1, 2, \ldots, m \\ g_i(x) = c_j, i = 1, 2, \ldots, n \end{array} \right\} \tag{14}$$

where x is the set of optimization variables and $f(x)$is the objective function. The constraint conditions, $h_i(x) \leq b_i$ and $g_i(x) = c_j$ are the inequality, and equality constraints respectively. The optimization problem describes the problem of finding an optimal x that minimizes $f(x)$ among all x satisfying the constraints. Convex optimization and nonconvex optimization are two important classes of optimization problems. In the convex problem, the objective function and the

inequality constraints function must be convex whereas the equality constraint function must be affine. The nonconvex problem deals with nonconvex objective function and/or constraints function.[185] A convex optimization problem is solved optimally by many efficient interior-point algorithms whereas nonconvex optimization problems are usually intractable so are approximated by convex problems to get the optimal solution.

In PLS, this objective function $f(x)$ is the considered performance metric, such as secrecy rate/capacity, SOP, power consumption, and secure energy efficiency. The optimization variable x may be the resources in the designs of the secure resource allocation, beamformer/precoder in beamforming and precoding, or element of antennas/cooperative nodes in the designs of antenna/node selection and cooperation. Following the great progress in theories and algorithms of optimization, the system designs in PLS has greatly benefited from recent advances to the point where optimization has now emerged as a major signal processing technique.

A detailed survey of the optimization approaches to enhance the PLS in the wireless communication system is provided by the authors in Reference 68. Quadratic programming is one of the optimization methods which involves the objective function having quadratic terms. Quadratic programming is used in the design problems of nonlinear programming. Some of the common quadratic problems in PLS are power minimization, secure power allocation, and beamforming. Another method used in PLS is SDP. It is used to optimize a linear function of variables under linear equality constraints and a non-negativity constraint. Most problems in PLS are usually non-convex, and they must be converted into convex problems using SDP. In turn, an efficient algorithm that is easy to implement is developed in order to obtain optimal performance metrics. One other optimization method is the difference of convex functions programming. In this, the objective function is the subtraction of two convex functions, widely used to solve problems of SR maximization. Furthermore, mixed-integer programming is one of the methods utilized. This method is applicable to problems that have discrete and continuous variables.

5.2 | Review of the optimization strategies in PLS

From the perspective of system designs ensuring PLS, mainly focus on the optimization of secure resource allocation, beamforming/precoding, and antenna/node selection and cooperation strategies. Table 7 summarizes the various methods used for the optimization of PLS performance measures.

5.2.1 | Secure resource allocation

The multidimensional wireless resources specifically containing frequency, timeslot, and power in OFDMA networks make it possible to intentionally extend the difference between the legitimate channel and the wiretap channel by secure resource allocation. In multi-antenna and multi-node wireless networks, the wireless resources generally refer to the spatial degrees of freedom provided by multiple antennas and nodes. However, because of the limited network resources, the main challenge of secure resource allocation is to utilize it efficiently to achieve the requirements of the performance metrics. Many works have focussed on two basic problems of secure resource allocation that are the subcarrier allocation and power allocation in multicarrier networks. In Reference 197, based on uplink transmission, the resource allocation problem for URLLC in real-time wireless control systems is studied. The problem is conducted by optimizing bandwidth

TABLE 7 Optimization methodology adopted in various literatures

Methodology	Reference	Performance metric optimized
Dual decomposition	186	SR
Mixed Integer programming	187-189	Power allocation
Alternating optimization	190	SOP
Successive convex approximation	191,192	SR
Semi-definite relaxation	192	SR
ZF-beamforming	193,194	Secrecy throughput
AN- beamforming	195,196	SR

and transmission power allocation in URLLC and control convergence rate subject to the constraints on communication and control. To formulate and solve the optimization problem, the authors first convert the control convergence rate requirement into a communication reliability constraint. Then, the co-design problem is replaced by a regular wireless resource allocation problem. By proving the converted problem is concave, an iteration algorithm is proposed to find the optimal communication resource allocation. Based on that, the optimal control convergence rate is obtained to optimize overall system performance. Two practical RSS methods are proposed in Reference 198 to transmit confidential messages, by constructing a random subcarrier set and performing a randomization procedure to achieve the secure precise wireless transmission per OFDM symbol. In Reference 199, the resource allocation for a secure multicarrier AF relay communication is studied where the optimization variable x is defined for the source and the relay respectively for specifying the state of communication on a specific carrier. For considering the fairness of resource allocation in secure multiuser OFDMA downlink works, the work presented in Reference 200 aims to assign sub-channels and allocate power to optimize the max-min fairness criterion over the users SR. An optimization problem for secure resource allocation and scheduling in OFDMA half-duplex DF relay-assisted networks is solved in Reference 186 by taking into account AN generation to combat a passive multiple antenna ED and the effects of imperfect CSIT in slow fading. The optimization problem is solved by dual decomposition which results in a highly scalable distributed iterative resource allocation algorithm. The packet data rate, secrecy data rate, power, and subcarrier allocation policies are optimized to achieve high outage performance. For D2D communications underlying cellular networks over the Nakagami-m fading channel presented in Reference 187, joint optimization of SINR thresholds and cellular user-D2D pairing optimization problem is formulated as mixed-integer non-linear programming. The sub-carrier allocation to different users, the relay assignments, and the power loading over different sub-carriers at transmitting nodes are optimized in Reference 188 for the dual-hop multiuser systems. The joint optimization problem is modeled as a mixed binary integer programming problem subject to exclusive sub-carrier allocation and separate power budget constraints at each node. In Reference 201, the solutions of the optimal relay power allocations for a massive MIMO DF relay network are derived for maximizing the secrecy outage capacity and minimizing the interception probability, respectively. The results in Reference 201 are expanded in Reference 190, in which to deal with the non-convexity of the joint node power and transmission time allocation problem, the approach of alternating optimization is addressed by maximizing over some of the variables and then maximizing over the rest. In Reference 191, authors have formulated an optimization problem to jointly design the trajectories and transmit power of UAV-base-station and UAV-Jammer in order to maximize the minimum average SR of the overall information receivers. Since the optimization problem is nonconvex and difficult to tackle directly so it is decomposed it into two sub-problems and then solved by employing an alternating iterative algorithm and the SCA technique. Authors in Reference 202 propose a new joint optimization framework to enhance the security performance by proactively controlling channel gains via adjusting the UAV trajectory in addition to applying the conventional power/rate adaptation, which leads to maximization of the average SR over a finite horizon, subject to the average and peak transmit power constraints as well as practical UAV's mobility constraints. Resource optimization problem to maximize the secrecy rate under the power and SOP constraints over parallel Rayleigh fading channel is investigated in Reference 203. In Reference 189, authors have jointly optimized the allocation of resource blocks and transmit power of fog computing-based IoT network with multiple devices, subject to respective QoS requirements, and the optimization problem is formulated as a mixed integer nonlinear programming problem to minimize the system energy consumption. An improved genetic algorithm is introduced to solve the problem.

5.2.2 | Secure beamforming and precoding

These are the signal processing techniques which are extensively exploited in wireless communication to ensure secure transmission. Secure beamforming typically refers to one-rank transmission by which only a single data stream is transmitted over multiple antennas or nodes, whereas secure precoding refers to multi-rank transmission by which more than one data streams can be transmitted at the same time.[204] The main idea of secure beamforming is to compute the optimal beamforming vector for achieving some performance metrics of PLS by enhancing the signal quality at the destination node and decreasing the signal quality at the eavesdropper. The beamforming design problem in PLS has been well investigated in many studies in the literature, with the aim of developing algorithms that minimize the interference and also maximize the secrecy of transmission. In Reference 205, authors have used semi-definite relaxation to obtain the optimal beamforming solution, which minimizes the transmission power subject to SINR constraints. In the paper, they showed that the quadratic optimization problems with non-convex and discontinuous constraints could be recast as SDP with

additional constraints, which imposes that the solution matrices must be of rank one. In Reference 193, using Taylor expansion, the optimization problem is solved. The author's study proved that their proposed algorithm outperformed both the signal-to-leakage-and-noise ratio-based algorithm and ZF beamforming. A new framework for the optimization of code rates in the SISOME channel is introduced in Reference 206 which does not require reliability or secrecy constraints within the wiretap channel. In this, main channel and ED channel are subjected to the quasi-static Rayleigh fading.

AN-assisted transmission is an effective way to utilize channel quality advantage in the transmission link. In this approach information-bearing signal and artificially generated noise is sent simultaneously over the channel. The generated noise is designed such that only the wiretap channel degrades while the main channel is kept intact. This concept was first realized by the authors in Reference 207. The information-bearing signal and the AN are injected into the range space and the null space of the legitimate user's channel matrix, respectively. In this manner, the artificial noise only deteriorates the ED but has a little detrimental impact on the legitimate receiver. However, to ensure that injected noise only affects the ED, the knowledge of CSI at the transmitter is required. The transmission of the AN is generally possible by using multiple antennas at the transmitter side or with the help of the relay nodes. This AN-based PLS scheme is further utilized by authors in References 208,209 to provide security for the multiple antenna system. Using a relay node for the AN injection is challenging because all the relay nodes must be perfectly synchronized. However, use of cooperative relay node is becoming a popular technique in providing security to IoT applications.[210] In Reference 211, authors have analyzed SOP of multiple cooperative jammers and multiple EDs using AN technique. Few remarkable works using relay nodes can be found in the literature.[212-214] In Reference 195, the AN-assisted beamforming is performed for degrading the ED channels while the optimal power allocation between the confidential information and AN is obtained in closed-form to minimize the secrecy rate outage probability. When only the location information of the ED is available at the source user, the location-based beamforming is optimally designed to minimize the SOP in Rician wiretap channels in Reference 215, while the resulting solution is extended to examine the solution of the optimal beamformer in the presence of a multi-antenna jammer in Reference 216. In Reference 196, for an AN-assisted secure transmission in the MIMOME wiretap channels, a joint power allocation and training overhead optimization problem for the maximization of effective SR is investigated. To solve the optimization problem in the MIMOME system, GSVD-based precoding can be implemented.[217] GSVD-based precoding decomposes transmitted channel matrices into several parallel sub-channels and confidential information is transmitted over sub-channels where the legitimate user is stronger than the ED. This method gives a closed-form solution for the achievable SR which is relatively fast and is asymptotically optimal at high SNRs. However, a rotation-based precoding algorithm for the MIMOME system is presented in Reference 218 which outperforms GSVD when the number of ED antennas is less than the transmitting antenna. The authors in Reference 194 considered the ZF criteria to define the beamforming vectors and investigated SR maximization problem to design the optimal power allocation strategy under three main constraints that is QoS requirements, SOP and maximum available power over the MISO NOMA network. The optimization of total transmission power under the constraints of minimum SR for NOMA-CR system assisted by SWIPT is studied in Reference 192. The solution to the optimization problem provided is based on the SCA algorithm and the semidefinite relaxation technique. For the MISO NOMA-CR authors in Reference 219 have investigated the optimal AN, power-splitting ratios, and transmission beamforming vectors for secondary users and EH users in order to minimize the transmission power of the secondary network. The constraints for the optimization problem are minimum SINR at the secondary users, minimum harvested energy by secondary users and EH users, maximum power at the secondary transmitter, and maximum permissible interference with licensed users. The proposed solution for the challenging non-convex optimization problem is based on the semidefinite relaxation method.

5.2.3 | Antenna/node selection and cooperation

To increase the achievable secrecy rate great efforts have been made for the optimization of the antenna/node selection and cooperation. Like, in multi-antenna diversity adopting a proper strategy of antenna selection, SR can be optimized. This concept is utilized in Reference 220, which concentrates on transmit antenna selection algorithm design based on branch and bound search in the massive MIMOME channels. In Reference 221, authors have proved that using linear precoding, the information leakage to the EDs can be sufficiently diminished, when the total number of available transmit antennas at the base station grows large, even when only a fixed number of them are selected. The cooperative nodes in the network offer two roles in the PLS of the system, cooperative relaying and cooperative jamming. PLS can be enhanced

by optimal selection of the relay nodes.[222,223] In Reference 224, authors use cooperative jamming to implement security for industrial wireless networks with mobile users and EDs. In the paper, they employed an edge computing device to intelligently select an optimal cooperative node. Another interesting study in Reference 210 implements this technique in IoT systems to enhance the PLS addressing a downlink transmission problem to handle multiple passive and non-colluding EDs. For a UAV-enabled cooperative jamming, a closed-form lower bound for the achievable SR, based on which the UAV's trajectory and transmit power are optimized alternately by an efficient iterative algorithm applying the block coordinate descent and successive convex optimization techniques in Reference 225. To maximize the covert transmission rate from the UAV to the legitimate ground user via optimizing the UAV's trajectory and transmit power, a new design framework is introduced in Reference 226, which utilizes SCA to develop an iterative algorithm. Using a UAV friendly jammer assisted by AN to enhance the NOMA-based IoT system having imperfect CSI is investigated in Reference 227. Apart from this hybrid strategy involving cooperative relaying and jamming is also widely explored in the literature[228,229] to optimize the secrecy performance. In Reference 230, authors design an optimal relay and jammer selection strategy where the ratio of received SNRs at the destination generated by any two relays is maximized. By applying the proposed strategy, computation complexity can be reduced. Also, the lower and upper bounds of the SOP expression based on the assumptions of existence of only illegitimate node is derived. In Reference 231, the SOP of a wireless powered communication network with an energy harvesting jammer is analyzed and minimized by optimizing the time allocation between the two phases of information transfer and energy transfer. For a multiuser multi-relay scenario for end-to-end secrecy rate, an optimization problem using dual decomposition is formulated in Reference 232 to jointly optimize power allocation at the base station, the relay selection, subcarrier assignment to users, and the power loading at each of the relaying node.

6 | RESULTS AND COMPARISONS

In this section, we present a summarized view of the computational complexity, implementation constraints, and generalization of the derived expressions and techniques over the fading channels. Table 8 provides a comparative study of the mathematical expressions of the various performance metric of the PLS over different fading channels derived in the published papers. This comparison makes the reader to understand the merits and demerits of the different mathematical representations that are used to define the performance parameters of the PLS over various fading channels in an effective manner.

Moreover, to shed light on the significance of implementing PLS in the emerging next-generation wireless applications to satisfy the security prerequisites and constraints by utilizing the specific characteristics of these applications is provided. In Table 9, application-based review is done, which reveals what are the basic necessity of security for a particular application scenario and how it is being achieved using PLS. It also explains the impact of the propagation scenarios on the performance metrics of the PLS.

7 | DISCUSSION AND FUTURE DIRECTIONS

From the previous sections, it is clear that the PLS has attracted the increasing concern of the researchers and some great work has already been done in this field. This work provides a comprehensive technical discussion on the state-of-the-art results on PLS, and its implementation over the various fading channels. This section provides the discussion and future directions to facilitate and inspire future research in analysis, design, optimization, and implementation of the physical security of wireless networks. The following open research challenges can be envisioned from the review done in the paper.

Security solution as the combination of PLS and cryptographic techniques: The ultra-reliable and low latency application of the next-generation network demand for ultra-strong security. The traditional cryptographic technique deployed at the higher layers of the transmission protocol stack involves computational complexity. PLS has the advantage of low complexity, and it is implemented on the physical layer of the transmission protocol. However, to satisfy the full-proof security demands of the emerging network, exploiting the characteristics of both types of security techniques can be thought of as a more exceptional solution.[235] To deploy such a technique, many challenging problems related to cross-layer analysis, secure coding schemes, hybrid encryption algorithms are required to be solved. In Reference 236, authors have presented an initial performance analysis of the PLS in conjunction with the cryptographic and proved that the combination of

TABLE 8 Expression representation of PLS performance metric over various fading Channels

Representation of the expression	Performance metric analyzed	Reference	Fading channel	Explanation
Meijer G function	SPSC	50	Weibull	The expressions presented in the mentioned paper are closed-form expressions in terms of the Meijer G function. Meijer G function is most widely used function to reduce the complex expressions into tractable expression. Major benefit of using this is that, it can be implemented easily in available software.
	SOP^L, SPSC	40	Generalized gamma	
	ASC, SOP, SOP^L	131	Generalized K	
	SOP, PNZ	95	Double shadowed Rician	
	SOP, PNZ	130	Co-related Nakagami-*m*/Gamma	
	ASC, SOP, SPSC	233	N-Nakagami	
	SOP	112	α-η-κ-μ	
EGBMGF	ASC, SOP, PNZ	43	Generalized K	This function is complex to implement but provides a more accurate analysis.
	ASC, SOP, SOP^L, SPSC	132	F-S	
	ASC, SOP	93	Cascaded fading channel	
EGBFHF	ASC	102	α-μ fading channel	Provides accurate analysis
	ASC	112	α-η-κ-μ	
Infinite series summation	ASC, SOP	84	Co- related Rayleigh	The expressions in terms of infinite series summation are required to be truncated to get the accurate results. So, using suitable measures, truncation error is required to be calculated.
	ASC, SOP, SOP^L	109	κ-μ	
	PNZ, SOP	96	Rayleigh/Rician	
	ASC, SOP, SPSC	114	B-X	
Bivariate Fox's H-function	Asymptotic SOP	103	SIMO α-μ	Using this, expressions are represented in closed-form. Although it is complex to implement but provide much accurate analysis.
	SOP	105	MIMO α-μ	
Gaussian Q function	SPSC	116	LN	Provides a simple analytical expression which can be implemented easily
Integral expression	SOP, ASC, SPSC	135	Weibull/LN	Solution to the complex integral expressions is not possible, so only lower bound analysis of the presented metrics is provided which does not lead to explicit analysis.
	SOP	234	Co-related Nakagami-*m*	

both techniques can be efficiently used to provide the overall security to the system. This work can be further studied over different propagation scenarios and the effectiveness of this approach can be explored in detail. The 5G and beyond network architecture presents heterogeneous features, where the communication nodes are deployed with dissimilar characteristics such as computing capacity, energy supply capacity, radio access technologies, protocol stack architecture, and so on. This requires that the combined security strategy designs must adapt to the heterogeneous architecture of networks, the variety of nodes, and the diversification of radio access technologies. So, the design of a simple, scalable but well-performing joint security scheme to trade-off between the performance and the complexity is an urgent need to be addressed.

PLS using IRS: In the scenarios of the spatially correlated communication link where the average power of the legitimate link is less than the average power of the ED link, the achievable secrecy capacity performance is degrading with the aforementioned techniques. Specifically, in such scenarios, the IRS is emerging as a promising key enabler to improve the PLS in an economical and energy-efficient manner.[237] IRS is a passive economical device[238] that can brilliantly reconfigure the wireless propagation conditions with the utilization of massive low-cost passive reflecting elements that are combined on a planar surface. In Reference 239, the IRS technique is explored for multi-antenna transmitter communicating with a single antenna receiver with a single antenna ED in between the path. In Reference 240, block coordinate descent and minorization algorithms are proposed to optimize the IRS-based PLS technique. Adding to this contribution[241,242] also investigates the optimization design techniques of the transmitters send beamforming and reflected beamforming at

TABLE 9 PLS in various application of wireless communication

Application	Reference	Contributions
D2D communication	148	Compares PLS performance metric for the cellular network and D2D communication system in the presence of multiple EDs
	149	SOP analysis for secrecy-based access control
	150	Proposes Kuhn-Munkres (KM) algorithm to increase the secrecy rate by the introduction of D2D communication under laying cellular network
	151	Derives an optimal joint power control solutions of both the cellular communication links and D2D pairs in terms of the cellular secrecy capacity and secrecy-based JPAC scheme with optimum D2D pair selection mechanism
	152	Derives secrecy rate for the D2D underlaid cellular network
IoT-based communication	153	Explains techniques to provide PLS in IoT-based communication network
	154	Proposes a ML-based antenna design to achieve directional communication between devices
	155	Proposes an energy-efficient transmission scheme suitable for resource constrained devices
	76	Presents a comprehensive survey on advances and challenges in resource-constrained secrecy coding and secret-key generation suitable for applications in the IoT
	156	Explains the features of physical layer key generation and physical layer encryption security techniques in IoT applications
VLC	159	Derives upper and lower bounds of the secrecy rate for the spatial modulation-based indoor VLC system
	161	Studies the impact of multiple reflections on the SOP considering multiple ED
	162	Derives SOP expression for the indoor VLC system with randomly distributed ED
	163	Analyzes SC of the SISO VLC system
	164	SOP and ESR for the multiuser VLC communication system
	159	SOP analysis for the VLC SWIPT system
UAV communication	167	Provides a comprehensive analysis of security system in UAV communication network
	168	Derives intercept probability expression for the eavesdropper
	169	Derives closed-form expression of SOP for A2A and A2G link for the randomly distributed ED
	170	Derives IP and ESR expression for single ED in urban environment
	171	Investigates the performance of secure connection probability for transmitting-to-jamming power ratio, the height of the UAVs and the UAV jammer location
V2V communication	173	Studies the relation between SC and the speed of a vehicle
	174	Impact of various vehicle, antenna and noise-related parameter on V2V communication is investigated
	175	Provides a study on various PLS protocols to achieve secrecy
	176	Studies the secrecy performance over cooperative vehicular AF network
BAN communication	180	Comparative SOP analysis of single-hop and multi-hop communication
	181	Proposes a simple lightweight encryption technique based on PLS
	182	Proposes multi-hop topology formation game to optimize multi-hop transmission in the uplink of a wireless BAN in terms of PLS and with delay constraints
	183	Proposes jamming-based technique to protect ED attack
	184	Proposes an ensured data provenance for body-worn devices utilizing spatial and temporal characteristics of wireless channel

IRS to maximize the secrecy rate in the legitimate communication link. Its distinguished features make it fit for providing security in the next-generation networks. However, the work on this is still in its infancy state and requires a further investigation to make the best utilization of the technique in the security paradigm of the wireless networks.

Implementation of PLS on various other services: Most of the recent wireless application scenario has its own QoS and security requirements. So, it is essential to rethink and redesign the PLS mechanism over the emerging applications such as eMBB and mMTC. In Reference 243, authors have presented techniques to improve the PLS in mMTC. However, to accommodate the rapidly changing technologies, it is required to design scalable security techniques that can adapt to the existing network. There is also an extensive scope of studying the PLS over fading channels that can be implemented to model these specific applications.

Analysis of non-traditional secrecy parameters: In the security paradigm, a promising future direction is to explore the various non-conventional PLS performance parameters such as GSOP, fractional equivocation, and information leakage rate over the various fading channels. The conventional outage performance does not distinguish between security and reliability. From a design perspective, these parameters provide an explicit measure of the security, which helps to design the transmission schemes to meet the required security measures of the new wireless communication network.

Investigation of physical layer authentication and physical layer key generation techniques in emerging technologies: Physical layer key generation provides an information-theoretic secure key generation solution.[244,245] An effective physical layer key generation and authentication scheme based on channel phase characteristics is investigated in Reference 246. The challenges and opportunities of the physical layer key generation over the 5G and beyond network are discussed in Reference 247. The application of this concept in the fields such as heterogeneous network, narrowband communication, and massive user connected network is still not much explored. In this sense, it can be considered as a subject for further investigation for developing a smart physical layer authentication mechanism.

ML-based channel estimation: PLS precoding schemes make an assumption of the knowledge or availability of the unintended user's CSI. This is the fundamental limitation of such PLS techniques. In practice it is very difficult for the transmitter to obtain the CSI of the ED. This is due to the fact that the ED does not naturally cooperate with the transmitter to send CSI feedback. The development of channel estimation techniques using deep learning has been investigated in References 248,249. From these investigations, it is evident that tackling imperfect CSI in PLS is one of the problems still open for research. The conventional channel estimation methods based on channel modeling have been proved to be insufficient for providing accurate and timely CSI. There has been a recent surge in research directed toward the feasibility of tackling some of the various communication problems using ML. In Reference 248, review of the rudimentary concepts of ML and its employment in the compelling applications of 5G networks, including cognitive radios, massive MIMOs, femto/small cells, heterogeneous networks, smart grid, EH, device-to- device communications are provided by the authors. Most of the research is devoted toward developing efficient and reliable algorithms for channel estimation in communication networks. The state-of-the-art of deep learning architectures and algorithms used for CSI acquisition and feedback for massive MIMO is presented in Reference 250. The recent development of deep learning-based wireless physical layers and several novel and efficient deep learning-based communication frameworks are investigated in Reference 251. In particular, focusing on 5G, three frameworks, NOMA, massive MIMO, and mmWave hybrid precoding based on deep learning are presented and their performances are investigated. However, it must be admitted that many technical implementations are in their infancy with open research questions, and it is a long road ahead to use the deep learning concepts to address wireless PLS issues thoroughly. ML has emerged as an effective tool for channel estimation in wireless communication systems, especially in some imperfect environments. The performance of the existing channel estimation algorithms can be augmented through the use of ML to achieve close-to-optimal algorithms with reduced complexity on the implementation. It is desirable to develop explainable deep learning methods that require to build the common data sets which may support in the field of wireless communication. So, scholars have a wide scope of entirely new research problems in the field of ML implemented in the wireless communication networks.

Overall optimization with security, reliability and throughput: To achieve the optimal network performance and user experience in a wireless network, the security, reliability, throughput, and delay should be considered jointly in system designs.[78] As these parameters interact with each other, consequently required to take into consideration for optimized system design. In general, physical layer secrecy constraints typically achieve at the expense of violating other specifications of the system. For instance, the reliability and throughput of the legitimate channel can be improved by increasing the transmission power which however may improve the capacity of the wiretap channel and increase the probability of successful eavesdropping. Likewise, although we can increase the coding rate at the transmitter for improving the security level while reducing the intercept probability, this leads to a decrease in transmission reliability, since a higher

coding rate may increase the OP of the intended channel. In order to achieve a near perfect system performance, the overall optimization with the joint considerations of security, reliability, and throughput is needed to be carried out, which may be challenging and intractable. For formulating and solving such complicated multi-objective problems, some convex/nonconvex optimization techniques and game theory, as well as stochastic geometry, are widely applied in this field.[252] In addition, currently and in the future energy efficiency of a network is attracting growing concerns. On imposing this criterion on the above discussed global optimization, the secure transmission designs will be extremely complicated work that calls for creative efforts to develop novel optimization theories and technologies.

8 | CONCLUSIONS

With the advancement in the new communication technologies, it is expected that in the near future, every device will be wirelessly connected. In such a scenario, data security will be a major requirement, which opens a broad scope for the research on the improvement of PLS in the system. In this paper, we have proposed a new framework for characterizing the current PLS over the fading channels based on computation and implementation complexity of the performance metrics. First, we have discussed the security requirements of the next-generation network, and based upon that, we have analyzed the advantages of PLS over the cryptographic approach. Then a comprehensive review of the PLS works has been provided with its classification based on fading model, ED, diversity techniques have been provided. Furthermore, a review of the optimization approaches adopted in PLS is presented. For understanding the importance of CSI and finite input signaling in PLS, a detailed review of the impact of both conditions is also provided. The application and implementation of PLS techniques in the emerging wireless communication network such as D2D, VLC, BAN, UAV, and IoT are comprehensively reviewed and discussed. Finally, this paper gives the reader a superior understanding of the advantages of the PLS and also provides a promising direction of the research over less explored non-conventional performance parameters such as GSOP, average information leakage rate, fractional equivocation. Due to the growing demand for the data traffic and emerging technologies to support it, researchers have a wide scope to explore the PLS over these networks.

CONFLICT OF INTEREST

Authors declare that there is no conflict of interest.

DATA AVAILABILITY STATEMENT

No data are available.

ORCID

Sandeep Kumar https://orcid.org/0000-0002-5750-6112

REFERENCES

1. Rappaport TS. *Wireless Communication - Principle and Practice*. Upper Saddle River, NJ: Prentice Hall PTR; 1996.
2. Shiu YS, Chang SY, Wu HC, Huang CH, Chen HH. Physical layer security in wireless networks: a tutorial. *IEEE Wirel Commun*. 2011;18(2):66-74.
3. Poor HV. Information and inference in the wireless physical layer. *IEEE Commun Mag*. 2012;19(1):40-47.
4. Stallings W. *Cryptography and Network Security:Principles and Practice*. New York, NY: Prentice Hall; 2008.
5. Hellman ME. An overview of public key cryptography. *IEEE Commun Mag*. 2002;16(6):42-49.
6. Schneier B. Description of a new variable-length key, 64-bit block cipher (blowfish). Paper presented at: Proceedings of the Fast Softw. Encryption Cambridge Security Workshop; 1993; Cambridge, UK.
7. Zhou X, Song L, Zhang Y. *Physical Layer Security in Wireless Communications*. Boca Raton, FL: CRC Press; 2014.
8. Agiwal M, Roy A, Saxena N. Next generation 5G wireless networks: a comprehensive survey. *IEEE Commun Surv Tutor*. 2016;18(3):1617-1655, thirdquarter.
9. He B, Zhou X. New physical layer security measures for wireless transmissions over fading channels. *IEEE Globecom*. Austin: IEEE; 2014:722-727.
10. Poor HV, Schaefer RF. Wireless physical layer security. *PNAS*. 2017;114(1):19-26.
11. Ö. Cepheli and G.K. Kurt, "Physical layer security in wireless communication networks," *Security, Privacy, Trust, and Resource Management in Mobile and Wireless*, IGI Global, Istanbul, Turkey: 2014, pp. 4666–4691.
12. Shanon CE. Communication theory of secrecy systems. *Bell Labs Techn J*. 1949;28(4):656-715.
13. Wyner AD. The wire-tap channel. *Bell Syst Tech J*. 1975;54(8):1355-1387.
14. Csiszar I, Korner J. Broadcast channels with confidential messages. *IEEE Trans Inf Theory*. 1978;24(3):339-348.

15. Bloch M, Barros J, Rodrigues MRD, McLaughlin SW. Wireless information-theoretic security. *IEEE Trans Inf Theory*. 2008;54(6):2515-2534.
16. Barros J, Rodrigues MRD. Secrecy capacity of wireless channels. Paper presented at: Proceedings of the IEEE International Symposium on Information Theory; 2006:356-360; Seattle, WA.
17. Gopala PK, Lai L, El Gamal H. On the secrecy capacity of fading channels. *IEEE Trans Inf Theory*. 2008;54(10):4687-4698.
18. Liu T, Lin P, Lin S, Hong Y-P, Jorswieck EA. To avoid or not to avoid CSI leakage in physical layer secret communication systems. *IEEE Commun Mag*. 2015;53(12):19-25.
19. He B, Zhou X, Abhayapala TD. Wireless physical layer security with imperfect channel state information: A survey. *ZTE Commun*. 2013;11(3):11-19.
20. Hyadi A, Rezki Z, Alouini M. An overview of physical layer security in wireless communication systems with CSIT uncertainty. *IEEE Access*. 2016;4:6121-6132.
21. Lai L, El Gamal H. The relay-eavesdropper channel: cooperation for secrecy. *IEEE Trans Inf Theory*. 2008;54(9):4005-4019.
22. Dong L, Han Z, Petropulur A, Poor HV. Improving wireless physical layer security via cooperating relays. *IEEE Trans Signal Process*. 2010;58(3):1875-1888.
23. Li Z, Yates R, Trappe W. Secure communication with a fading eavesdropper channel. Paper presented at: Proceedings of the IEEE International Symposium on Information Theory; 2007; Nice, France.
24. Rezki Z, Alomair B, Alouini M. On the secrecy capacity of the MISO wiretap channel under imperfect channel estimation. Paper presented at: Proceedings of the IEEE Global Communication Conference (GLOBECOM), Austin, USA; December 2014.
25. Zhou X, Rezki Z, Alomair B, Alouini M. Achievable rates of secure transmission in gaussian MISO channel with imperfect main channel estimation. *IEEE Trans Wirel Commun*. 2016;15(6):4470-4485.
26. Love DJ, Heath RW, Lau VKN, Gesbert D, Rao BD, Andrews M. An overview of limited feedback in wireless communication systems. *IEEE J Sel Areas Commun*. 2008;26(8):1341-1365.
27. Hyadi A, Rezki Z, Alouini M. On the secrecy capacity of the multiple-antenna wiretap channel with limited CSI feedback. Paper presented at: Proceedings of the IEEE Information Theory Workshop (ITW), San Diego, CA; September 2016:1-6.
28. Lin P, Jorswieck E. On the fast fading Gaussian wiretap channel with statistical channel state information at the transmitter. *IEEE Trans Inf Foren Sec*. 2016;11(1):46-58.
29. Mukherjee P, Ulukus S. Fading wiretap channel with no CSI anywhere. Paper presented at: Proceedings of the IEEE International Symposium on Information Theory; July 2013:1347-1351; Istanbul, Turkey.
30. Liu T, Mukherjee P, Ulukus S, Lin S, Hong YP. Secure degrees of freedom of MIMO rayleigh block fading wiretap with no CSI anywhere. *IEEE Trans Wirel Comm*. 2015;14(5):2655-2668.
31. Brante G, Alves H, Souza RD, Latva-aho M. Secrecy analysis of transmit antenna selection cooperative schemes with no channel state information at the transmitter. *IEEE Trans Commun*. 2015;63(4):1330-1342.
32. Pinto PC, Barros J, Win MZ. Secure communication in stochastic wireless networks—Part I: connectivity. *IEEE T Inf Foren Sec*. 2012;7(1):125-138.
33. Huang C, Chang T, Zhou X, Hong YP. Two-way training for discriminatory channel estimation in wireless MIMO systems. *IEEE Trans Signal Process*. 2013;61(10):2724-2738. https://doi.org/10.1109/TSP.2013.2245124.
34. Tugnait JK. Pilot spoofing attack detection and countermeasure. *IEEE Trans Commun*. 2018;66(5):2093-2016.
35. Li J, Petropulu AP, Poor HV. Cooperative transmission for relay networks based on second-order statistics of channel state information. *IEEE Trans Signal Process*. 2011;59(3):1280-1291.
36. Hu J, Yan S, Zhou X, Shu F, Li J. Covert wireless communications with channel inversion power control in Rayleigh fading. *IEEE Trans Veh Technol*. 2019;68(12):12135-12149. https://doi.org/10.1109/TVT.2019.2949304.
37. Shahzad K, Zhou X, Yan S, Covert communication in fading channels under channel uncertainty. Paper presented at: Proceedings of the 2017 IEEE 85th Vehicular Technology Conference (VTC Spring); 2017:1-5; Sydney, NSW. https://doi.org/10.1109/VTCSpring.2017.8108525.
38. Yan S, He B, Zhou X, Cong Y, Swindlehurst AL. Delay-intolerant covert communications with either fixed or random transmit power. *IEEE T Inf Foren Sec*. 2019;14(1):129-140. https://doi.org/10.1109/TIFS.2018.2846257.
39. Bloch M, Barros J. *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge, MA: Cambridge University Press; 2011.
40. Zhang H, Ansari IS, Gao C, Guo Y, Lei H. On physical layer security over generalized gamma fading channels. *IEEE Commun Lett*. 2015;19(7):1257-1260.
41. Liu X. Outage probability of secrecy capacity over correlated log-Normal fading channels. *IEEE Commun Lett*. 2013;17(2):289-292.
42. Sarkar MZI, Ratnarajah T, Sellathurai M. Secrecy capacity of Nakagami-m fading wireless channels in the presence of multiple eavesdroppers. Paper presented at: Proceedings of the Conference Record of the 43rd Asilomar Conference on Signals, Systems and Computers; 2009; Pacific Grove, CA.
43. Lei H, Ansari IS, Gao C, Guo Y, Pan G, Qaraqe KA. Physical-layer security over generalised-K fading channels. *IET Commun*. 2016;10(16):2233-2237.
44. Moualeu JM, da Costa DB, Hamouda W, Dias US, de Souza RAA. Physical layer security over α-κ-μ and α-η-μ fading channels. *IEEE Trans Veh Technol*. 2019;68(1):1025-1029.
45. Bhargav N, Cotton SL. Secrecy capacity analysis for α-μ/κ-μ and κ-μ/α-μ fading scenarios. Paper presented at: Proceedings of the IEEE 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC); 2016:1-6; Valencia.

46. He B, Zhou X, Swindlehurst AL. On secrecy metrics for physical layer security over quasi-static fading channels. *IEEE Trans Wirel Commun*. 2016;15(10):6193-6924.
47. Zhou X, McKay MR, Maham B, Hjørungnes A. Rethinking the secrecy outage formulation:a secure transmission design perspective. *IEEE Commun Lett*. 2011;15(3):302-304.
48. Alves H, Tomé MD, Nardelli PH, De Lima CH, Latva-Aho M. Enhanced transmit antenna selection scheme for secure throughput maximization without csi at the transmitter,ε *IEEE Access*, vol. 4, pp. 4861–4873, 2016.
49. Zhao H, Yang L, Pan G, Alouini M. Secrecy outage analysis over fluctuating two-ray fading channels. *Electron Lett*. 2019;55(15):866-868.
50. Liu X. Probability of strictly positive secrecy capacity of the Weibull fading channel. Paper presented at: Proceedings of the IEEE Global Communications Conference (GLOBECOM); 2013; Atlanta, GA.
51. Pan G, Tang C, Zhang X, Li T, Weng Y, Chen Y. Physical-layer security over non-small-scale fading channels. *IEEE Trans Veh Technol*. 2015;65(3):1326-1339.
52. Liu X. Probability of strictly positive secrecy capacity of the Rician-Rician fading channel. *IEEE Wirel Commun Lett*. 2013;2(1):50-53.
53. Kong L, Kaddoum G, Chergui H. On physical layer security over Fox's H-function wiretap fading channels. *IEEE Trans Veh Technol*. 2019;68(7):6608-6621.
54. Cheffena M, Mathur A, Lei H, Ai Y. On physical layer security of double Rayleigh fading channels for vehicular communications. *IEEE Wirel Commun Lett*. 2018;7(6):1038-1041.
55. Liu X. Average secrecy capacity of the Weibull fading channel. Paper presented at:Proceedings of the13th IEEE Annual Consumer Communications & Networking Conference (CCNC); 2016; Las Vegas, NV.
56. Raghava GD, Rajan BS. Secrecy capacity of the Gaussian wiretap channel with finite complex constellation input; January 2010 [Online]. http://arxiv.org/abs/1010.1163.
57. Rodrigues MRD, Somekh Bharuch A, Bloch M. On Gaussian wiretap channels with M-PAM inputs. Paper presented at: Proceedings of the EWConference, Lucca, Italy; April 2010:774-781.
58. Aghdam SR, Nooraiepour A, Duman TM. An Overview of Physical Layer Security With Finite-Alphabet Signaling. *IEEE Commun Surv & Tuts*. 2019;21(2):1829-1850.
59. Ouyang C, Wu S, Jiang C, Ng DWK, Yang H. Secrecy performance for finite-alphabet inputs over fluctuating two-ray channels in FDA communications. *IEEE Wirel Commun Lett*. 2020;9(10):1638-1642.
60. Zhang Y, Zhang J, Yu H. Physically securing energy-based massive MIMO MAC via joint alignment of multi-user constellations and artificial noise. *IEEE J Select Areas Commun*. 2018;36(4):829-844.
61. Xia G, Lin Y, Liu T, Shu F, Hanzo L. Transmit antenna selection and beamformer design for secure spatial modulation with rough CSI of eve. *IEEE Trans Wirel Commun*. 2020;19(7):4643-4656.
62. Xia G, Shu F, Zhang Y, Wang J, ten Brink S, Speidel J. Antenna selection method of maximizing secrecy rate for green secure spatial modulation. *IEEE Trans Green Commun Netw*. 2019;3(2):288-301.
63. Yan S, Zhou X, Yang N, He B, Abhayapala TD. Artificial-noise-aided secure transmission in wiretap channels with transmitter-side correlation. *IEEE Trans Wirel Commun*. 2016;15(12):8286-8297.
64. Liu Y, Chen HH, Wang L. Physical layer security for next generation wireless networks: theories, technologies, and challenges. *IEEE Commun Surv Tuts*. 2017;19(1):347-376.
65. Wu Y, Khisti A, Xiao C, Caire G, Wong K, Gao X. A survey of physical layer security techniques for 5G wireless networks and challenges ahead. *IEEE J Select Areas Commun*. 2018;36(4):679-695.
66. Sun L, Du Q. Physical layer security with its applications in 5G networks: a review. *China Commun*. 2017;14(12):1-14.
67. Yang N, Wang L, Geraci G, Elkashlan M. Safeguarding 5g wireless communication networks using physical layer security. *IEEE Commun Mag*. 2015;53(4):20-27.
68. Wang D, Bai B, Zhao W, Han Z. A survey of optimization approaches for wireless physical layer security. *IEEE Commun Surv Tutor*. 2019;21(2):1878-1911.
69. Obeed M, Salhab AM, Alouini M, Zummo SA. Survey on physical layer security in optical wireless communication systems. Paper presented at: Proceedings of the 7th International Conference on Communications and Networking (ComNet); 2018:1-5; Hammamet,Tunisia.
70. Arfaoui MA, Soltani MD, Tavakkolnia I. Physical layer security for visible light communication systems: a survey. https://arxiv.org/abs/1905.11450.
71. Mukherjee A, Fakoorian SAA, Huang J, Swindlehurst AL. Principles of physical layer security in multiuser wireless networks: a survey. *IEEE Commun Surv Tutor*. 2014;16(3):1550-1573.
72. Rodriguez LJ, Tran NH, Duong TQ, Le-Ngoc T. Physical layer security in wireless cooperative relay networks: state of the art and beyond. *IEEE Commun Mag*. 2015;53(12):32-39.
73. Kapetanovic D, Zheng G, Rusek F. Physical layer security for massive MIMO: an overview on passive eavesdropping and active attacks. *IEEE Commun Mag*. 2015;53(6):21-27.
74. Hamamreh JM, Furqan HM, Arslan H. Classifications and applications of physical layer security techniques for confidentiality: a comprehensive survey. *IEEE Commun Surv Tutor*. 2019;21(2):1773-1828.
75. Zou Y, Zhu J, Wang X, Leung V. Improving physical-layer security in wireless communications using diversity techniques. *IEEE Netw*. 2015;29(1):42-48.
76. Mukherjee A. Physical-layer security in the internet of things: sensing and communication confidentiality under resource constraints. *Proc IEEE*. 2015;103(10):1747-1761.

77. Sun L, Du Q. A review of physical layer security techniques for internet of things: challenges and solutions. *Entropy*. 2018;20(10):1-21.
78. Zou Y, Zhu J, Wang X, Hanzo L. A survey on wireless security:technical challenges, recent advances and future trends. *Proc IEEE*. 2016;104(9):1727-1765.
79. Kumar S. Performance of ED based spectrum sensing over α–η–μ fading channel. *Wirel Pers Commun*. 2018;100(4):1845-1857.
80. Kumar S, Kaur M, Singh NK, Singh K, Chauhan PS. Energy detection based spectrum sensing for gamma shadowed α–η–μ and α–κ–μ fading channels. *AEU-Int J Electron C*. 2018;93:26-31. https://doi.org/10.1016/j.aeue.2018.05.031.
81. Kumar S. Energy detection in Hoyt/gamma Fading Channel with micro-diversity reception. *Wirel Pers Commun*. 2018;101:723-734.
82. Shankar PM. *Fading and Shadowing in Wireless Systems*. 1st ed. New York, NY: Springer; 2012.
83. Jeon H, Kim N, Choi J, Lee H, Ha J. Bounds on secrecy capacity over correlated ergodic fading channels at high SNR. *IEEE Trans Inf Theory*. 2011;57(4):1975-1983.
84. Sun X, Zhao C, Jiang M. Closed-form expressions for secrecy capacity over correlated rayleigh fading channels; July 2020. https://arxiv.org/abs/1003.4355.
85. Zhu J, Jiang X, Takahashi O, Shiratori N. Secrecy capacity of correlated rayleigh fading channels. Paper presented at: Proceedings of the 18th Asia-Pacific Conference on Communications (APCC); 2012:333-337; Jeju Island.
86. Tang J, Dabaghchian M, Zeng K, Wen H. Impact of mobility on physical layer security over wireless fading channels. *IEEE Trans Wirel Commun*. 2018;17(12):7849-7864.
87. Khodadoust AM, Hodtani GA. Physical layer security in shotgun cellular systems over correlated/independent shadow fading channels. *Ann Telecommun*. 2020;75:253-267.
88. Belmoubarik S, Aniba G, Elgraini B. Secrecy capacity of a Nakagami-m fading channel in the presence of cooperative eavesdroppers. Paper presented at: Proceedings of the Mediterranean Microwave Symposium; 2014:1-6; Marrakech.
89. Omri A, Hasna MO. Average secrecy outage rate and average secrecy outage duration of wireless communication systems with diversity over Nakagami-m fading channels. *IEEE Trans Wirel Commun*. 2018;17(6):3822-3833.
90. Vuppala S, Abreu G, Ratnarajah T, Liu W. Secrecy outage in correlated nakagami-m. *IEEE PIMRC*. Washington, DC: IEEE; 2014:145-149.
91. Ha DB, Van PT, Vu TT. Physical layer secrecy performance analysis over Rayleigh/Nakagami fading channels. Paper presented at: Proceedings of the World Congress on Engineering and Computer Science; Vol II 2014:1-6; San Francisco.
92. Sarkar MZI, Ratnarajah T. Secure communication through Nakagami-m fading MISO channel. *IEEE ICC*. Kyoto, Japan: IEEE; 2011:1-5.
93. Ata SÖ. Secrecy performance analysis over cascaded fading channels. *IET Commun*. 2019;13(2):59-264.
94. Tang C, Pan G, Li T. Secrecy outage analysis of underlay cognitive radio unit over Nakagami- m fading channels. *IEEE Wirel Commun Lett*. 2014;3(6):609-612.
95. Ai Y, Kong L, Cheffena M. Secrecy outage analysis of double shadowed Rician channels. *IET Digit Lib*. 2019;55(13):765-767.
96. Ha D, Duong TQ, Tran D, Zepernick H, Vu TT. Physical layer secrecy performance over Rayleigh/Rician fading channels. Paper presented at: Proceedings of the International Conference on Advanced Technologies for Communications (ATC 2014); 2014:113-118; Hanoi.
97. da Costa DB, Yacoub MD. Average Channel capacity for generalized fading scenarios. *IEEE Commun Lett*. 2007;11(12):949-951.
98. Rasethuntsa TR, Kumar S. An integrated performance evaluation of ED-based spectrum sensing over α − κ−μ and α − κ−μ—extreme fading channels. *Trans Emerg Telecommun Technol*. 2019;30(5):e3569.
99. Rasethuntsa TR, Kaur M, Kumar S. On the outage probability and BER of a DF-based multi-hop system over α–κ–μ and α–κ–μ-extreme fading channels. *AEU-Int J Electron C*. 2020;124:153324. https://doi.org/10.1016/j.aeue.2020.153324.
100. Rasethuntsa TR, Kaur M, Kumar S, Chauhan PS, Singh K. On the performance of DF-based multi-hop system over α − κ − μ and α − κ − μ-extreme fading channels. *Digit Signal Process*. 2021;109:102909. https://doi.org/10.1016/j.dsp.2020.102909.
101. Kong L, Tran H, Kaddoum G. Performance analysis of physical layer security over α–μ fading channel. *Electron Lett*. 2016;52(1):45-47.
102. Lei H, Ansari IS, Pan G, Alomair B, Alouini MS. Secrecy capacity analysis over α- μ fading channels. *IEEE Commun Lett*. 2017;21(6):1445-1448.
103. Kong L, Kaddoum G, Rezki Z. Highly accurate and asymptotic analysis on the SOP over SIMO α−μ fading channels. *IEEE Commun Lett*. 2018;22(10):2088-2091.
104. Kong L, Kaddoum G, Vuppala S. On secrecy analysis for D2D networks over α − μ fading channels with randomly distributed eavesdroppers. Paper presented at: Proceedings of the IEEE ICC Workshop 5G-Security; 2018:1-6; Kansas City.
105. Kong L, Vuppala S, Kaddoum G. Secrecy analysis of random MIMO wireless networks over α-μ fading channels. *IEEE Trans Veh Tech*. 2018;67(12):654-666.
106. Kong L, Kaddoum G, da Costa DB. Cascaded α − μ fading channels: reliability and security analysis. *IEEE Access*. 2018;6:41 978-41 992.
107. Bhargav N, Cotton SL, Simmons DE. Secrecy capacity analysis over k− μ fading channels: theory and applications; 2020. https://arxiv.org/pdf/1506.08606.pdf.
108. Iwata S, Ohtsuki T, Kam PY. Secure outage probability over κ − μ fading channels. Paper presented at: Proceedings of the IEEE International Conference Communications (ICC); 2017:1-6; Paris, France.
109. Moualeu JM, Hamouda W. On the secrecy performance analysis of SIMO systems over κ-μ fading channels. *IEEE Commun Lett*. 2017;21(11):2544-2547.
110. Fraidenraich G, Yacoub MD. The α-η-μ and α-κ-μ fading distributions. Paper presented at: Proceedings of the IEEE 9th International Symposium Spread Spectrum Techniques and Applications, Manaus, Brazil; August 2006:16-20.
111. Yacoub MD. The α-η-κ-μ fading model. *IEEE Trans Antennas Propag*. 2016;64(8):3597-3610.
112. Mathur A, Ai Y, Bhatnagar MR, Cheffena M, Ohtsuki T. On physical layer security of α-η-κ-μ fading channels. *IEEE Commun Lett*. 2018;22(10):2168-2171.

113. Kaur M, Yadav R. Performance analysis of Beaulieu-Xie fading channel with MRC diversity reception. *Trans Oon Emerg Telecommun Technol*. 2020;31(7):e3949.
114. Chauhan PS, Kumar S, Soni SK. On the physical layer security over Beaulieu-Xie fading channel. *AEU-Int J Electron C*. 2020;113:152940. https://doi.org/10.1016/j.aeue.2019.152940.
115. Singh R, Soni SK, Verma PK, Kumar S. Performance analysis of mrc combiner output in log normal shadowed fading International Conference on Computing, Communication & Automation; 2015:1116-1120.
116. Liu X. Secrecy capacity of wireless links subject to log-Normal fading. Paper presented at: Proceedings of the 7th International Conference on Communications and Networking; 2012; China, Kun Ming.
117. Liu X. Strictly positive secrecy capacity of log-normal fading channel with multiple eavesdroppers. Paper presented at: Proceedings of the IEEE International Conference on Communications (ICC); 2014; Sydney, NSW.
118. Liu X. Outage probability of secrecy capacity over correlated log-Normal fading channels. *IEEE Commun Lett*. 2013;17(2):289-292.
119. Sarkar MZI, Ratnarajah T. Secrecy capacity over log-normal fading channel with diversity combining techniques. Paper presented at: Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC); 2013; Shanghai.
120. Kumar S, Soni SK, Jain P. Micro-diversity analysis of error probability and channel capacity over Hoyt-gamma fading. *Radio Eng*. 2017;26(4):1096-1103.
121. Yadav P, Kumar R, Kumar S. Effective capacity analysis over generalized lognormal shadowed composite fading channels. *Internet Technol Lett*. 2020;3:e171. https://doi.org/10.1002/itl2.171.
122. Sofotasios PC, Tsiftsis TA, Van KH, Freear S, Wilhelmsson LR, Valkama M. The kappa-mu /IG composite statistical distribution in RF and FSO wireless channels. Paper presented at: Proceedings of the IEEE 78th Vehicular Technology Conference (VTC Fall); 2013:1-5; Las Vegas, NV.
123. Yadav P, Kumar S, Kumar R. Analysis of EC over gamma shadowed α-η-μ Fading Channel. Paper presented at: Proceedings of the IOP Conference Series: Materials Science and Engineering; 2021; AP, India.
124. Kumar S, Chauhan PS, Raghuwanshi P, Kaur M. ED performance over α-η-μ/IG and α-κ-μ/IG generalized fading channels with diversity reception and cooperative sensing: a unified approach. *AEU-Int J Electron C*. 2018;97:273-279. https://doi.org/10.1016/j.aeue.2018.10.027.
125. Yadav P, Kumar S, Kumar R. Effective capacity analysis over α-κ-μ/gamma composite fading channel. Paper preseneted at: 2020 2nd International Conference on Advances in Computing, Communication Control and Networking (ICACCCN), Greater Noida, India; 2020:587-592; Noida, India, https://doi.org/10.1109/ICACCCN51052.2020.9362859.
126. J. Sun, X. Li, M. Huang, Y. Ding, J. Jin and G. Pan, εPerformance analysis of physical layer security over k-μ shadowed fading channels,ε *IET Commun, vol*. 12. 8, pp. 970–975, 2018.
127. Jiang-Feng S, Xing-Wang L, Yuan D, Jian-He D. Physical layer security over SIMO κ-μ shadowed fading channels. *Recent Adv Electr Electron Eng*. 2019;13:871-878. https://doi.org/10.2174/2352096512666191108094202.
128. Muralikrishnan S, Kalyani S. Secrecy capacity of κ-μ shadowed fading channels. *IEEE Commun Lett*. 2018;22(8):1728-1731.
129. Lopez-Martinez FJ, Romero-Jerez JM, Paris JF. On the calculation of the incomplete MGF with applications to wireless communications. *IEEE Trans Commun*. 2017;65(1):458-469.
130. Alexandropoulos GC, Peppas KP. Secrecy outage analysis over correlated composite Nakagami-m/gamma fading channels. *IEEE Commun Lett*. 2018;22(1):77-80.
131. Lei H, Gao C, Ansari IS, Guo Y, Pan G, Qaraqe KA. On physical-layer security over SIMO generalized- K fading channels. *IEEE Trans Veh Technol*. 2016;65(9):7780-7785.
132. Al-Hamood H, Al-Raweshidy HS. Security performance analysis of physical layer over fisher-Snedecor fading channels; July 2018. https://arxiv.org/abs/1805.07652.
133. Kong L, Kaddoum G. On physical layer security over the fisher- Snedecor F wiretap fading channels. *IEEE Access*. 2018;6:39466-39472.
134. Singh R, Soni SK, Raw RS, Kumar S. A new approximate closed-form distribution and performance analysis of a composite Weibull/log-Normal Fading Channel. *Wirel Pers Commun*. 2016;92:883-900. https://doi.org/10.1007/s11277-016-3583-3.
135. Singh R, Rawat M. Performance analysis of physical layer security over Weibull/lognormal composite fading channel with MRC reception. *AEU-Int J Electron C*. 2019;110:152849.
136. Moualeu JM, da Costa DB, Hamouda W, Dias US, de Souza RAA. Physical layer security over α-κ-μ and α-η-μ fading channels. *IEEE Trans Veh Technol*. 2019;68:1025-1029.
137. Wang J, Liu C, Wang J, Dai J, Lin M, Chen M. Secrecy outage probability analysis over Malaga-Malaga fading channels. Paper presented at: Proceedings of the IEEE International Conference on Communications (ICC); 2018:1-6; Kansas City.
138. Lin S-H, Lu R-R, Fu X-T, Tong A-L, Wang J-Y. Physical-layer security analysis over M-distributed fading channels. *Entropy*. 2019;21(10):1-19.
139. Bjelaković I, Boche H, Sommerfeld J. Strong secrecy in arbitrarily varying wiretap channels. Paper presented at: Proceedings of the IEEE Information Theory Workshop; 2012; Lausanne.
140. Boche H, Cai M, Deppe C, Notzel J. Classical-quantum arbitrarily varying wiretap channel: secret message transmission under jamming attacks. Paper presented at: Proceedings of the IEEE International Symposium on Information Theory (ISIT); 2017; Aachen.
141. Liu X. Outage probability of secrecy capacity over correlated log-Normal fading channels. *IEEE Commun Lett*. 2013;17(2):289-292.
142. Zhou Y, Zhu J, Wang X, Leung VCM. Improving physical-layer security in wireless communications using diversity techniques. *IEEE Network*. 2015;29(1):42-48.

143. Mukherjee A, Swindlehurst AL. Robust Beamforming for security in MIMO wiretap channels with imperfect CSI. *IEEE Trans Signal Process*. 2011;59(1):351-361.
144. Zheng G, Choo L, Wong K. Optimal cooperative jamming to enhance physical layer security using relays. *IEEE Trans Signal Process*. 2011;59(3):1317-1322.
145. Chraiti M, Ghrayeb A, Assi C, Hasna MO. On the achievable secrecy diversity of cooperative networks with untrusted relays. *IEEE Trans Commun*. 2018;66(1):39-53.
146. Gao Y, Ge J, Gao H. Physical layer security with maximal ratio combining over heterogeneous $\kappa-\mu$ and $\eta-\mu$ fading channels. *Wirel Pers Commun*. 2016;86:1387-1400.
147. Kumar S et al. On the spectrum sensing of gamma shadowed Hoyt fading channel with MRC reception. *J Electromagnet Waves Appl*. 2018;32(16):1-10.
148. Zhu D, Swindlehurst AL, Fakoorian SAA, Xu W, Zhao C. Device-to-device communications: the physical layer security advantage. Paper presented at: Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP); 2014:1606-1610; Florence.
149. Yue J, Ma C, Yu H, Zhou W. Secrecy-based access control for device-to-device communication Underlaying cellular networks. *IEEE Commun Lett*. 2013;17(11):2068-2071.
150. Zhang H, Wang T, Song L, Han Z. Radio resource allocation for physical-layer security in D2D underlay communications. Paper presented at: Proceedings of the IEEE ICC, Sydney, NSW; 2014:2319-2324; Australia.
151. Zhang R, Cheng X, Yang L. Joint power and access control for physical layer security in D2D communications underlaying cellular networks. Paper presented at: Proceedings of the IEEE ICC; 2016:1-6; Kuala Lumpur, Malaysia.
152. Xu H, Pan C, Xu W, Shi J, Chen M, Heng W. Improving wireless physical layer security via D2D communication. Paper presented at: Proceedings of the IEEE Global Communications Conference (GLOBECOM); 2018:1-7; Abu Dhabi, United Arab Emirates.
153. Sun L, Du Q. A review of physical layer security techniques for internet of things: challenges and solutions. *Entropy*. 2018;20:730. https://doi.org/10.3390/e20100730.
154. Hong T, Liu C, Kadoch M. Machine learning based antenna design for physical layer security in ambient backscatter communications. *Wirel Commun Mob Comput*. 2019;2019:1-10. https://doi.org/10.1155/2019/4870656.
155. Shang X, Liu A, Wang Y, Xie Q, Wang Y. Energy-efficient transmission based on direct links:toward secure cooperative internet of things. *Wirel Commun Mob Comput*. 2018;2018:1-8. https://doi.org/10.1155/2018/5012096.
156. Zhang J, Duong TQ, Woods R, Marshall A. Securing wireless Communications of the Internet of things from the physical layer, an overview. *Entropy*. 2017;19(8):1–16. https://doi.org/10.3390/e19080420.
157. Pecorella T, Brilli L, Mucchi L. The role of physical layer security in IoT: a novel perspective. *Information*. 2016;7(3):1–17.
158. Wang N, Wang P, Alipour-Fanid A, Jiao L, Zeng K. Physical-Layer Security of 5G Wireless Networks for IoT: Challenges and Opportunities. *IEEE Internet of Things Journal*. 2019;6(5):8169–8181.
159. Ge H, Dai J, Huang B, Wang J. Secrecy rate analysis for visible light communications using spatial modulation. Paper presented at: Proceedings of the IEEE 21st International Conference on High Performance Computing and Communications; IEEE 17th International Conference on Smart Conference on Data Science and Systems (HPCC/SmartCity/DSS); 2019:1241-1248; Zhangjiajie, China.
160. Qiu Y, Wang J, Lin S, Wang J, Lin M. Secrecy outage probability analysis for visible light communications with SWIPT and random terminals. 11th International Conference on Wireless Communications and Signal Processing (WCSP); 2019:1-6; Xi'an, China.
161. Cho S, Chen G, Chun H, Coon JP, O'Brien D. Impact of multipath reflections on secrecy in VLC systems with randomly located eavesdroppers. Paper presented at: Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC); 2018:1-6; Barcelona.
162. Cho S, Chen G, Coon JP. Secrecy analysis in visible light communication systems with randomly located eavesdroppers. Paper presented at: Proceedings of the IEEE International Conference on Communications Workshops (ICC Workshops), Paris, France; 2017:475-480; IEEE
163. Wang JY, Liu C, Wang JB, Wu Y, Lin M, Cheng J. Physical layer security for indoor visible light communications: secrecy capacity analysis. *IEEE Trans Commun*. 2018;66(12):6423-6436.
164. Yin L, Hass H. Physical-layer security in multiuser visible light communication networks. *IEEE J Sel Areas Commun*. 2018;36(1):162-174.
165. Odido D, Madara D. Emerging technologies: use of unmanned aerial Systems in the Realisation of vision 2030 goals in the counties. *Int J Appl Sci Technol*. 2013;3(8):107-127.
166. Matolak DW. Unmanned aerial vehicles: communications challenges and future aerial networking. Paper presented at: Proceedings of the International Conference on Computing, Networking and Communications (ICNC); 2015:567-572; Garden Grove, CA.
167. Sun X, Ng DWK, Ding Z, Xu Y, Zhong Z. Physical layer security in UAV systems: challenges and opportunities. *IEEE Wirel Commun*. 2019;26(5):40-47.
168. Zhou Y, Yeoh PL, Chen H, et al. Improving physical layer security via a UAV friendly jammer for unknown eavesdropper location. *IEEE Trans Veh Technol*. 2018;67(11):11280-11284.
169. Ye J, Zhang C, Pan G, Chen Y, Ding Z. Secrecy analysis for spatially random UAV systems. Paper presented at: Proceedings of the IEEE Globecom Workshops (GC Wkshps), Abu Dhabi, United Arab Emirates; 2018:1-6.
170. Bao T, Yang H, Hasna MO. Secrecy performance analysis of UAV-assisted relaying communication systems. *IEEE Trans Veh Technol*. 2020;69(1):1122-1126.
171. Tang J, Chen G, Coon JP. Secrecy performance analysis of UAV transmissions subject to eavesdropping and jamming, August 2018, https://arxiv.org/abs/1808.08628.

172. Ameen HA, Mahamad AK, Saon S, Nor DM, Ghazi K. A review on vehicle to vehicle communication system and applications. *Indones J Electr Eng Comput Sci*. 2020;18(1):188-198.
173. Ahn NY, Lee D, Oh SJ. Vehicle Communication Using Secrecy Capacity. In: Arai K., Bhatia R., Kapoor S. (eds) Proceedings of the Future Technologies Conference (FTC) 2018. FTC 2018. Advances in Intelligent Systems and Computing, vol 881. Springer, Cham. https://doi.org/10.1007/978-3-030-02683-7_13.
174. Kargl F, Papadimitratos P, Buttyan L, et al. Secure vehicular communication systems: implementation, performance, and research challenges. *IEEE Commun Mag*. 2018;46(11):110-118.
175. ElHalawany BM, El-Banna AAA, Wu K. Physical-layer security and privacy for vehicle-to-everything. *IEEE Commun Mag*. 2019;57(10):84-90.
176. Pandey A, Yadav S. Physical layer security for cooperative vehicular amplify-and-forward relay networks. Paper presented at: Proceedings of the Conference on Information and Communication Technology (CICT); 2018:1-6; Jabalpur,India.
177. Han D, Bai B, Chen W. Secure V2V communications via relays: resource allocation and performance analysis. *IEEE Wirel Commun Lett*. 2017;6(3):342-345.
178. Ahn N-Y. Physical layer security of autonomous driving: secure vehicle-to-vehicle communication in a security cluster. *Ad hoc Sens Wirel Netw*. 2020;45:293-336.
179. Dharshini S, Subashini MM. An overview on wireless body area networks. *Innovations in Power and Advanced Computing Technologies (i-PACT)*. Vellore; IEEE; 2017:1-10.
180. Niu H, Sun L, Ito M, Sezaki K. Secure transmission through multihop relaying in wireless body area networks. Paper presented at: Proceedings of the IEEE 3rd Global Conference on Consumer Electronics (GCCE); 2014:395-396; Tokyo.
181. Dautov R, Tsouri GR. Securing while sampling in wireless body area networks with application to electrocardiography. *IEEE J Biomed Health Inform*. 2016;20(1):135-142.
182. Moosavi H, Bui FM. Delay-aware optimization of physical layer security in multi-hop wireless body area networks. *IEEE T Inf Foren Sec*. 2016;11(9):1928-1939.
183. Halevi T, Saxena N. Acoustic eavesdropping attacks on constrained wireless device pairing. *IEEE T Inf Foren Sec*. 2013;8(3):563-577.
184. Ali ST, Sivaraman V, Ostry D, Tsudik G, Jha S. Securing first-hop data provenance for Bodyworn devices using wireless link fingerprints. *IEEE T Inf Foren Sec*. 2014;9(12):2193-2204.
185. Boyad S, Vandenberghe L. *Convex Optimization*. Cambridge, UK: Cambridge University Press; 2004.
186. Ng DWK, Lo ES, Schober R. Secure resource allocation and scheduling for OFDMA decode-and-forward relay networks. *IEEE Trans Wirel Commun*. 2011;10(10):3528-3540. https://doi.org/10.1109/TWC.2011.082011.110538.
187. Lu B, Lin S, Shi J, Wang Y. Resource allocation for D2D communications underlaying cellular networks over Nakagami- m fading channel. *IEEE Access*. 2019;7:21816-21825. https://doi.org/10.1109/ACCESS.2019.2894721.
188. Aman W, Sidhu GAS, Jabeen T, Gao F, Jin S. Enhancing physical layer security in dual-hop multiuser transmission. Paper presented at: Proceeding of the IEEE Wireless Communications and Networking Conference, Doha, Qatar; 2016:1:6. https://doi.org/10.1109/WCNC.2016.7564989.
189. Li X, Liu Y, Ji H, Zhang H, Leung VCM. Optimizing resources allocation for fog computing-based internet of things networks. *IEEE Access*. 2019;7:64907-64922.
190. Chen J, Chen X, Gerstacker WH, Ng DWK. Resource allocation for a massive MIMO relay aided secure communication. *IEEE Trans Inf Foren Sec*. 2016;11(8):1700-1711.
191. Zhou X, Wu Q, Yan S, Shu F, Li J. UAV-enabled secure communications: joint trajectory and transmit power optimization. *IEEE Trans Veh Technol*. 2019;68(4):4069-4073.
192. Zhou F, Chu Z, Sun H, Hu RQ, Hanzo L. Artificial noise aided secure cognitive beamforming for cooperative MISO-NOMA using SWIPT. *IEEE J Select Areas Commun*. 2018;36(4):918-931.
193. Zhao P, Zhang M, Yu H, Luo H, Chen W. Robust beamforming design for sum secrecy rate optimization in MU-MISO networks. *IEEE T Inf Foren Sec*. 2015;10(9):1812-1823.
194. Wang H, Zhang X, Yang Q, Tsiftsis TA. Secure users oriented downlink MISO NOMA. *IEEE J Select Top Signal Process*. 2019;13(3):671-684. https://doi.org/10.1109/JSTSP.2019.2899778.
195. Xiong J, Wong K-K, Ma D, Wei J. A closed-form power allocation for minimizing secrecy outage probability for MISO wiretap channels via masked beamforming. *IEEE Commun Lett*. 2012;16(9):1496-1499.
196. Wang H, Wang C, Ng DWK. Artificial noise assisted secure transmission under training and feedback. *IEEE Trans Signal Process*. 2015;63(23):6285-6298.
197. Chang B, Zhang L, Li L, Zhao G, Chen Z. Optimizing resource allocation in URLLC for real-time wireless control systems. *IEEE Trans Veh Technol*. 2019;68(9):8916-8927. https://doi.org/10.1109/TVT.2019.2930153.
198. Shen T, Zhang S, Chen R, et al. Two practical random-subcarrier-selection methods for secure precise wireless transmissions. *IEEE Trans Veh Technol*. 2019;68(9):9018-9028. https://doi.org/10.1109/TVT.2019.2931751.
199. Jindal A, Bose R. Resource allocation for secure multicarrier AF relay system under total power constraint. *IEEE Commun Lett*. 2015;19(2):231-234.
200. Karachontzitis S, Timotheou S, Krikidis I, Berberidis K. Security-aware max-min resource allocation in multiuser OFDMA downlink. *IEEE Trans Inf Foren Sec*. 2015;10(3):529-542.
201. Chen J, Chen X, Gerstacker W. Optimal power allocation for a massive MIMO relay aided secure communication. Paper presented at: Proceedings of the IEEE Global Communications Conference (GLOBECOM); February 2015:1-6; San Diego, CA.

202. Zhang G, Wu Q, Cui M, Zhang R. Securing UAV communications via joint trajectory and power control. *IEEE Trans Wirel Commun*. 2019;18(2):1376-1389.
203. Laurenti N, Tomasin S, Renna F. Resource allocation for secret transmissions on parallel Rayleigh channels. Paper presented at: Proceedings of the 2014 IEEE International Conference on Communications (ICC); 2014:2209-2214; Sydney, NSW.
204. Hong YWP, Kuo CCJ. Enhancing physical-layer secrecy in multiantenna wireless systems: an overview of signal processing approaches. *IEEE Signal Process Mag*. 2013;30(5):29-40.
205. Huang Y, Palomar DP. Rank-constrained separable Semidefinite programming with applications to optimal Beamforming. *IEEE Trans Signal Process*. 2010;58(2):664-678.
206. Yan S, Yang N, Geraci G, Malaney R, Yuan J. Optimization of code rates in SISOME wiretap channels. *IEEE Trans Wirel Commun*. 2015;14(11):6377-6388.
207. Negi R, Goel S. Secret communication using artificial noise. Paper presented at: Proceedings of the 2005 IEEE 62nd Vehicular Technology Conference VTC-2005-Fall; 2005:1906-1910; Dallas, TX.
208. Zhou X, McKay MR. Secure transmission with artificial noise over fading channels: achievable rate and optimal power allocation. *IEEE Trans Veh Technol*. 2010;59(8):3831-3842.
209. Romero-Zurita N, Ghogho M, McLernon D. Outage probability based power distribution between data and artificial noise for physical layer security. *IEEE Signal Process Lett*. 2012;19(2):71-74.
210. Hu L, Wen H, Wu B, et al. Cooperative jamming for physical layer security enhancement in internet of things. *IEEE Internet Things J*. 2018;5(1):219-228.
211. Cumanan K, Alexandropoulos GC, Ding Z, Karagiannidis GK. Secure communications with cooperative jamming: optimal power allocation and secrecy outage analysis. *IEEE Trans Veh Technol*. 2017;66(8):7495-7505.
212. Goeckel D, Vasudevan S, Towsley D, Adams S, Ding Z, Leung K. Artificial noise generation from cooperative relays for everlasting secrecy in two-hop wireless networks. *IEEE J Sel Areas Commun*. 2011;29(10):2067-2078.
213. Tang X, Liu R, Spasojević P, Poor HV. Interference-assisted secret communication. Paper presented at: Proceedings of the IEEE Information Theory Workshop (ITW), Porto, Portugal; May 2008; 164-168.
214. Vilela JP, Bloch M, Barros J, McLaughlin SW. Wireless secrecy regions with friendly jamming. *IEEE Trans Inf Forens Sec*. 2011;6(2):256-266.
215. Yan S, Malaney R. Location-based beamforming for enhancing secrecy in Rician wiretap channels. *IEEE Trans Wirel Commun*. 2016;15(4):2780-2791.
216. Liu C, Malaney R. Location-based beamforming and physical layer security in Rician wiretap channels. *IEEE Trans Wirel Commun*. 2016;15(11):7847-7857.
217. Fakoorian SAA, Swindlehurst AL. Optimal power allocation for GSVD-based beamforming in the MIMO Gaussian wiretap channel. Paper presented at: Proceedings of the IEEE International Symposium on Information Theory (ISIT), Cambridge, MA; 2012:2321-2325.
218. Zhang X, Qi Y, Vaezi M. A rotation-based method for precoding in Gaussian MIMOME channels; 2021. https://arxiv.org/abs/1908.00994. Accessed January 2021.
219. Garcia CE, Camana MR, Koo I. Joint beamforming and artificial noise optimization for secure transmissions in MISO-NOMA cognitive radio system with SWIPT. *Electronics*. 2020;9:1948. https://doi.org/10.3390/electronics9111948.
220. Ouyang C, Ou Z, Zhang L, Yang H. Optimal transmit antenna selection algorithm in massive MIMOME channels. 2019 IEEE Wireless Communications and Networking Conference (WCNC); 2019:1-6; Marrakesh, Morocco, https://doi.org/10.1109/WCNC.2019.8886342
221. Bereyhi A, Asaad S, Muller RR, Schaefer RF, Rabiei AM. On robustness of massive MIMO systems against passive eavesdropping under antenna selection. Paper presented at: Proceeding of the IEEE Global Communications Conference (GLOBECOM); 2018; Abu Dhabi, United Arab Emirates.
222. Zou Y, Wang X, Shen W. Optimal relay selection for physical layer security in cooperative wireless networks. *IEEE J Sel Areas Commun*. 2013;31(10):2099-2111.
223. Huang Y, Al-Qahtani FS, Duong TQ, Wang J. Secure transmission in MIMO wiretap channels using general-order transmit antenna selection with outdated CSI. *IEEE Trans Commun*. 2015;63(8):2959-2971.
224. Zhang T, Wen H, Tang J, Song H, Xie F. Cooperative jamming secure scheme for IWNs random Mobile users aided by edge computing intelligent node selection. *IEEE Trans Ind Inform*. 2020;1. https://doi.org/10.1109/TII.2020.3017767.
225. Li A, Wu Q, Zhang R. UAV-enabled cooperative jamming for improving secrecy of ground Wiretap Channel. *IEEE Wirel Commun Lett*. 2019;8(1):181-184.
226. Zhou X, Yan S, Hu J, Sun J, Li J, Shu F. Joint optimization of a UAV's trajectory and transmit power for covert communications. *IEEE Trans Signal Process*. 2019;67(16):4276-4290. https://doi.org/10.1109/TSP.2019.29.
227. Chen Y, Zhang Z, Li B. Enhancing physical layer security via a UAV friendly jammer for NOMA-based IoT systems with imperfect CSI. *Trans Emerg Telecommun Technol*. 2021;32(3):e4175. https://doi.org/10.1002/ett.4175.
228. Wang C, Wang H-M, Xia X-G. Hybrid opportunistic relaying and jamming with power allocation for secure cooperative networks. *IEEE Trans Wirel Commun*. 2015;14(2):589-605.
229. Wang H-M, Luo M, Yin Q, Xia X-G. Hybrid cooperative beamforming and jamming for physical-layer security of two-way relay networks. *IEEE Trans Inf Foren Sec*. 2013;8(12):2007-2020.
230. Li G, Sheng X, Wu J, Yu H. Securing transmissions by friendly jamming scheme in wireless networks. *J Parall Distrib Comput*. 2020;144:260-267.

231. Moon J, Lee H, Song C, Lee I. Secrecy outage minimization for wireless powered communication networks with an energy harvesting jammer. Paper presented at: Proceedings of the IEEE Global Communications Conference (GLOBECOM); December 2016:1-5; Washington, DC.
232. W. Aman, G. Ahmad, S. Sidhu, Haji M. Furqan, Zain Ali, "Enhancing physical layer security in AF relay–assisted multicarrier wireless transmission," *Trans Emerg Telecommun Technol*, Vol. 29, no. 6, 2018. e3289.
233. Xu L, Yu X, Wang H, et al. Physical layer security performance of mobile vehicular networks. *Mob Netw Appl*. 2020;25:643-649.
234. Liu W, Vuppala S, Abreu G, Ratnarajah T. Secrecy outage in correlated nakagami-m fading channels. Paper presented at: Proceedings of the IEEE PIMRC; 2014:145-149; Washington, DC.
235. Robyns P, Quax P, Lamotte W. PHY-layer security is no alternative to cryptography. Paper presented at: Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Network, Boston Massachusetts; July 2017; 160-162.
236. Mucchi L, Nizzi F, Pecorella T, Fantacci R, Esposito F. Benefits of physical layer security to cryptography: tradeoff and applications. Paper presented at: Proceedings of the IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom); 2019:1-3; Sochi, Russia.
237. Zhao J, Liu Y. A survey of intelligent reflecting surfaces (IRSs):towards 6G wireless communication networks; August 2019. https://arxiv.org/pdf/1907.04789.pdf.
238. Wu Q, Zhang R. Towards smart and reconfigurable environment: intelligent reflecting surface aided wireless network. *IEEE Commun Mag*. 2020;58(1):106-112.
239. Cui M, Zhang G, Zhang R. Secure Wireless Communication via Intelligent Reflecting Surface. *IEEE Wirel Commun Lett*. 2019;8(5):1410-1414.
240. Yu X, Xu D, Schober R. Enabling secure wireless communications via intelligent reflecting surfaces; August 2020. https://arxiv.org/abs/1904.09573.
241. Shen H, Xu W, Gong S, He Z, Zhao C. Secrecy rate maximization for intelligent reflecting surface assisted multi-antenna communications. *IEEE Commun Lett*. 2019;23(9):1488-1492.
242. Chen J, Liang YC, Pei Y, Guo H. Intelligent reflecting surface:a programmable wireless environment for physical layer security. *IEEE Access*. 2019;7:82599-82612.
243. C. Bockelmann, Pratas N, Nikopour H, Au K, Svensson T, Stefanovic C, Popovski P, Dekorsy A. Massive machine-type communications in 5G: physical and MAC-layer solutions,ε *IEEE Commun Mag*, vol. 54, no. 9, pp. 59–65, 2016.
244. Ren K, Su H, Wang Q. Secret key generation exploiting channel characteristics in wireless communications. *IEEE Wirel Commun*. 2011;18(4):6-12.
245. Zai K. Physical layer key generation in wireless networks: challenges and opportunities. *IEEE Commun Mag*. 2015;53:33-39.
246. Cheng L, Zhou L, Seet BC, Li W, Ma D, Wei J. Efficient physical-layer secret key generation and authentication schemes based on wireless channel-phase. *Mob Inf Syst*. 2017;2017:1-13. https://doi.org/10.1155/2017/7393526.
247. Li G. Physical layer key generation in 5G and beyond wireless communications: challenges and opportunities. *Entropy*. 2019;21(5):48-54.
248. Jiang C, Zhang H, Ren Y, Han Z, Chen K, Hanzo L. Machine learning paradigms for next-generation wireless networks. *IEEE Wirel Commun*. 2017;24(2):98-105.
249. Otoum Y, Liu D, Nayak A. DL-IDS: a deep learning–based intrusion detection framework for securing IoT. *Trans Emerg Telecommun Technol*. 2019;e3803:1–14. https://doi.org/10.1002/ett.3803.
250. Mashhadi B, Gündüz D. Deep learning for massive MIMO Channel state acquisition and feedback. *J Indian Inst Sci*. 2020;100:369-382.
251. Huang H, Guo S, Gui G, et al. Deep learning for physical-layer 5G wireless techniques: opportunities, challenges and solutions. *IEEE Wirel Commun*. 2020;27(1):214-222.
252. Zhang N, Cheng N, Lu N, Zhang X, Mark JW, Shen X. Partner selection and incentive mechanism for physical layer security. *IEEE Trans Wirel Commun*. 2015;14(8):4265-4276.

How to cite this article: Yadav P, Kumar S, Kumar R. A comprehensive survey of physical layer security over fading channels: Classifications, applications, and challenges. *Trans Emerging Tel Tech*. 2021;e4270. https://doi.org/10.1002/ett.4270