HOSTED BY

ELSEVIER

Contents lists available at ScienceDirect

Engineering Science and Technology, an International Journal

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

Review

Key less physical layer security for wireless networks: A survey

Megha. S. Kumar, R. Ramanathan [*], M. Jayakumar

Department of Electronics and Communication Engineering, Amrita School of Engineering, Coimbatore, Amrita Vishwa Vidyapeetham, India

ARTICLE INFO

Article history:
Received 6 May 2021
Revised 28 July 2022
Accepted 7 September 2022
Available online 23 September 2022

Keywords:
Physical layer security
Keyless security
Channel coding
Beamforming
Artificial noise
Wireless communication

ABSTRACT

Physical layer security (PLS) has become the kernel concept for ensuring wireless network security. The main goal of this treatise is to provide a systematic classification of key less schemes. We have classified key less PLS into code, channel adaptation and artificial noise (AN) based approaches and carried out a survey of the diverse schemes employed in literature for key less approach. Further, we have provided the advantages, observations and future directions for each of the techniques. Industry 4.0 revolution with the Internet of Things (IoT) is going to rule the next wireless era with its promising smart home, smart health care, smart retail to name a few. Therefore, we have provided a discussion on the application of key less PLS in IoT. Further, we also discuss about two emerging areas that can be employed for enhancing PLS such as Intelligent Reflecting Surface (IRS) and Artificial Intelligence (AI). We have also provided some of the existing security challenges in the IoT application scenario. We have also presented the open research challenges and future directions in the area of key less PLS.

Contents

1. Introduction

The wireless medium exposes the information to several passive and active attacks due to its broadcast nature. Conventional cryptographic techniques such as Diffie Hellman key exchange [1], discrete logarithm [2] among many others, involve complex mathematical computations which the adversary may not be able to perform with ease, as the time involved in cracking the secret code could be much higher than the data validity. However, in future, the security provided by such schemes could be cracked because of the development of quantum computers and there is a flurry of ongoing research in the area of quantum cryptography.

Moreover, traditional schemes will not hold long because of the complex key management infrastructure requirement. Quantum cryptography [3] does not use public key, instead, the technique

[*] Corresponding author.
E-mail address: r_ramanathan@cb.amrita.edu (R. Ramanathan).

https://doi.org/10.1016/j.jestch.2022.101260
2215-0986/

Table 1
Summary of abbreviations.

Abbreviations	Notations
AN	Artificial Noise
AI	Artificial Intelligence
AFF	Artificial Fast Fading
AO	Alternating Optimization
ASC	Average Secrecy Capacity
BER	Bit Error Rate
BS	Base Station
BAN	Body Area Network
BCH	Bose-Chaudhuri-Hocquenghem
BC–CM	Broadcast Channel with Confidential Message
CSI	Channel State Information
CES	Collusive Eavesdropping Scheme
CJ	Cooperative Jamming
CP	Cyclic Prefix
CS	Cognitive Security
C-AmBC	Cognitive Ambient Backscatter Communication Technology
CPS	Cyber Physical Systems
DM	Directional Modulation
DL	Deep Learning
D2D	Device to Device
DNN	Deep Neural Network
FDD	Frequency Division Duplexing
FP	Fractional Programming
GST	Generalized Selection Transmission
GFDM	Generalized Frequency Division Multiplexing
HARQ	Hybrid Automatic Repeat Request protocol
HetNets	Heterogeneous Networks
IoT	Internet of Things
IA	Interference Alignment
IC–CM	Interference Channels with Confidential Message
IRS	Intelligent Reflecting Surface
ITS	Intelligent Transportation System
LDPC	Low Density Parity Check
LOS	Line of Sight
MAC-WTC	Multiple Access for Wiretap Channel
MISO	Multiple Input Single Output
MMSE	Minimum Mean Square Error
mmWave	Millimeter Wave
mMTC	Massive Machine Type Communication
MO	Manifold Optimization
MRC	Maximal Ratio Combining
NOMA	Non Orthogonal Multiple Access
OFDM	Orthogonal Frequency Division Multiplexing
OTFS	Orthogonal Time Frequency Space
OTDM	Orthogonal Transform Division Multiplexing
OFDM-SIS	Orthogonal Frequency Division Multiplexing with Subcarrier Index Selection
OSTBC	Orthogonal Space Time Block Code
PER	Packet Error Rate
PLS	Physical Layer Security
PAPR	Peak to Average Power Ratio
POSTBC	Precoded Orthogonal Space Time Block Code
PMI	Precoding Matrix Indicator
QoS	Quality of Service
RBF	Randomized Beamforming
RIS	Reconfigurable Intelligent Surfaces
SCLDGM	Serially Concatenated Low Density Generator Matrix
SNR	Signal to Noise Ratio
SARA	Secrecy Adaptation and Rate Adaptation
SOP	Secrecy Outage Probability
SINR	Signal to Interference Plus Noise Ratio
SWIPT	Simultaneous Wireless Information and Power Transfer
TDD	Time Division Duplexing
TBF	Transmit Beamforming
UFMC	Universal Filtered Multicarrier
UAV	Unmanned Aerial Vehicle
URLLC	Ultra Reliable Low Latency Communication
V-MIMO	Virtual Multiple Input Multiple Output
VLC	Visible Light Communication
VPL	Vehicle Penetration Loss
VANET	Vehicular Adhoc Network
V2X	Vehicle to Everything
WPT	Wireless Power Transfer

relies on the laws of quantum theory, such as Heisenberg's uncertainty principle, for sharing the secret between two end points. Recently, the concept of Physical Layer Security (PLS) [4–6] or information-theoretic security has emerged as an alternative to traditional crypto schemes and there is a flurry of research in this area as well. The underlying idea for PLS has been put forth in their seminal works by Shannon [7] and Wyner [8]. Shannon considered noiseless communication systems and shared key for securing systems. Wyner put forth the concept of wiretap channel model wherein, the eavesdropper's channel is assumed to have low Signal to Noise Ratio (SNR) than the legitimate channel. However, practically, the notion of a completely noiseless system is an ideal case, eavesdropper's channel can be less noisier than legitimate link and sharing of secret keys can have a lot of security risks. Hence, devising algorithms for securing wireless networks is the need of the hour. PLS techniques can be broadly classified into key based and key less schemes. The principles involved in key based PLS schemes for wireless networks [9–12] are, channel reciprocity, temporal and spatial variations. Channel reciprocity indicates that, the effect of multipath fading on either ends of the same link are identical. The variations in the temporal domain is brought in because of the mobility of transmitter, receiver or any object in the area and spatial decorrelation means that, the channel between two distinct nodes will be unique and an adversary at a third location experiences uncorrelated channel. Therefore, the adversary may not be able to obtain similar Channel State Information (CSI) as the legitimate nodes, resulting in distinct keys for the legitimate pair and adversary. 1 provides the abbreviations used in this work. In our work, we have carried out a systematic investigation of key less PLS schemes. Employing key less approaches to secure wireless networks has a lot of advantages. There is no requirement of key sharing and can be employed for both Time Division Duplexing (TDD) and Frequency Division Duplexing (FDD) systems unlike key based PLS schemes. When it comes to computational burden, most of the processing is only at the transmitter side. Practically, key less schemes can achieve perfect secrecy. These reasons served as the major motivation for exploring the various key less PLS approaches researched so far. An elaborate classification of key less PLS is very lean. Therefore, we have classified key less security based on the methods by which the scheme can be implemented, such as code, channel variation and AN based approaches. The commonly used metrics to analyse the performance of key less schemes are, secrecy capacity or secrecy rate, Secrecy Outage Probability (SOP), secrecy throughput and security gap. Security gap can be analysed from Bit Error Rate (BER) or Packet Error Rate (PER). Secrecy capacity is defined as the channel capacity difference between legitimate and adversary channels. This metric was further extended as SOP for analysing the secrecy of fading environments. Secrecy capacity provides achievable bounds by taking into consideration the random channel behaviour but may not provide the actual secrecy performance. Therefore, the probability of error such as BER and PER between Bob's and Eve's channel is considered as a better metric for obtaining practical secrecy performance. There are different notions for secrecy such as perfect secrecy, ideal secrecy, weak secrecy, strong secrecy, distinguishing secrecy and semantic secrecy. In this manuscript, in contrast to the existing surveys, we present the recent approaches for key less PLS to aid the readers in understanding the current developments in the area of key less PLS. Further, Internet of Things (IoT) being a widely researched and fast growing domain with a lot of application scenarios under it, we forsee the need of security here. Therefore, in this manuscript, we have also presented a discussion on the various recent works that explore the possibility of key less PLS in IoT. Apart from this, a discussion on other emerging areas such as Artificial Intelligence (AI) and Intelligent Reflecting Surface (IRS) for PLS are also presented. PLS schemes are applied in a variety

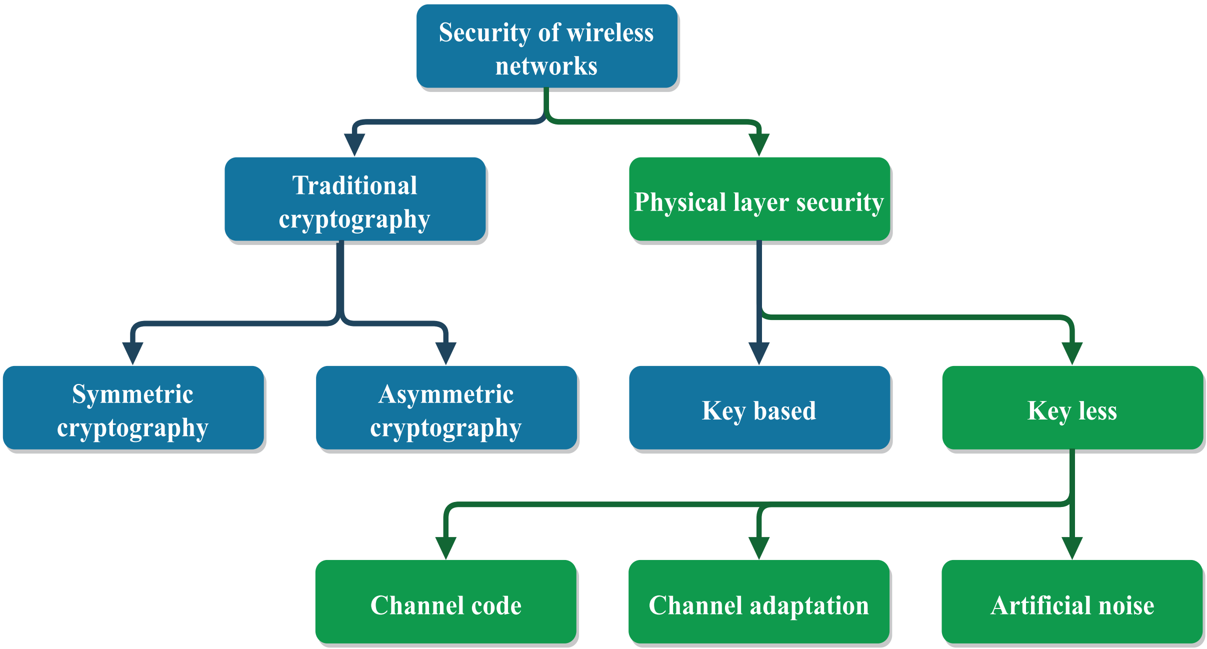

Fig. 1. Classification of wireless network security.

of applications namely Visible Light Communication (VLC), Unmanned Aerial Vehicles (UAVs), Body Area Network (BAN), IoT, Device to Device communication (D2D), Radio Frequency Identification (RFID), Millimeter Wave communication (mmWave), Massive Machine Type Communication (mMTC), Vehicular Adhoc Networks (VANET), Non Orthogonal Multiple Access (NOMA) systems to name a few. 1 depicts the broad classification of PLS schemes. The schemes discussed in this work are highlighted in green colour in 1. Major highlights of this work include,

1. A thorough analysis and classification of key less PLS schemes.
2. Provides the advantages, observations and future directions for all the schemes.
3. Identifies the performance metrics used to evaluate each scheme.
4. Identifies the various recent techniques under each scheme.
5. Presents a discussion on other emerging areas such as IRS for PLS and AI for PLS.
6. Explores the scope of key less PLS in IoT.

The manuscript is organized as follows, 2 describes the various approaches for key less PLS. In 3, we provide the application of key less PLS in the context of IoT. 4 provides a discussion on the open research challenges and future directions in key less PLS. Finally, 5 concludes the manuscript.

2. Approaches for key less PLS

In this section, we have classified key less PLS based on implementation and enhancement approaches. To implement key less PLS, there are mainly three approaches namely channel code, channel adaptation and AN whereas to enhance PLS, we have presented two hot topics of research, i.e. AI and IRS.

2.1. Approaches to implement key less PLS

Here, we have presented the different ways to implement key less PLS. The classification of key less PLS into channel code, channel adaptation and AN based approaches rely on the fact that, all the three schemes i.e. channel coding, channel adaptation and AN are Signal to Interference plus Noise Ratio (SINR) based approaches. Providing secrecy is achievable when Eve's SINR is naturally lower than Bob's SINR due to channel quality or artificially lower due to any particular approach. In channel codes, we have discussed various codes such as Low Density Parity Check (LDPC), polar, lattice, convolutional and hybrid codes that are employed to enhance security of the physical layer. In channel adaptation and AN based approaches, schemes developed in time, frequency and spatial domains are investigated. It is to be noted that, channel code, adaptation and AN approaches have its own merits and demerits when employed for ensuring security. Merits, we have already discussed in the introduction. The differences are as follows, in the case of channel coding, it is necessary that the SINR of Bob is higher than that of Eve. In the case of channel adaptation, Eve should have higher fading than Bob and the technique is susceptible to channel errors. AN injection is also challenged by issues such as susceptibility to channel errors as in the case of channel adaptation, might result in increased Peak to Average Power Ratio (PAPR), a lot of power resources are given up in the process. Also, AN requires a lot more degrees of freedom at the transmitter than at Bob.

2.1.1. Channel coding

When adversary channel is degraded than legitimate channel, error control codes [13] play a major role in ensuring security of wireless systems. For instance, randomized coding scheme [14]. The LDPC [15,16] codes are extensively used for enhancing secrecy capacity of wiretap channels. However, its application in randomized coset coding [17] scheme for gaussian wiretap channel as illustrated in 2, requires a practical decoder. Hence, a Serially Concatenated Low Density Generator Matrix [18] (SCLDGM) concatenated with convolutional codes is employed. Joint iterative message passing algorithm is considered for realizing the decoder. The scheme is analysed using BER metric of Bob and Eve. The highest desirable BER at Bob and the lowest desirable BER at eavesdropper gives two distinct SNRs measured as dB. The difference between these SNR values gives the secrecy capacity. The SCLDGM scheme gives a very small security gap of 1dB. In [16], authors explore coded modulation methods, to produce security against

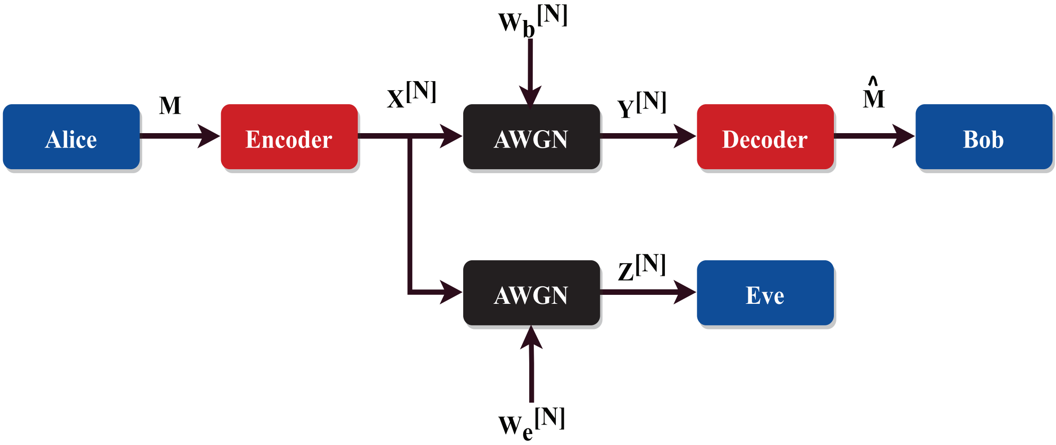

Fig. 2. Gaussian wiretap channel [26].

wiretaps as well as availability for the intended user. A multilayer coding method is specifically taken into account. The constellation's impact on the security achieved is evaluated, with a focus on its dimensionality and cardinality. It is inferred that, using multi-level code can cut the growing security gap by several decibels. Savings can be achieved further by tailoring the utilised code's distribution of puncturing to a particular constellation of the specific signal. Designing finite length LDPC codes for gaussian wiretap channel is a challenging issue. Hence, the performance of finite length LDPC in gaussian wiretap channels is studied by [19], with the aim of investigating the regions of capacity-equivocation. Further, to optimize code for the considered metrics, a twofold code optimization tool is also developed. Another set of codes used in literature for enhancing security are polar codes [20,21]. In [21], the authors propose a scheme that combines Dragonfly and Water Cycle Algorithms. The final transmission block of private bits is where the noise is introduced. Only authorised receivers are capable of accurately decoding the sensitive information from the transmitter since they are aware of the positions of the secret bits and the jamming position, where noise is being injected. Information is entirely jammed, so the eavesdropper is unaware of the jamming position and sensitive bits. As a result, the sent signal is unclear to the listener. For multiuser scenario, practical coding schemes are not available. Hence, [22], proposed a polar coding scheme by taking into account polar coding for asymmetric channel and universal polar coding. The proposed scheme is designed to attain secrecy capacity for a general wiretap channel. Further, the scheme determines the best-known inner bounds for multiuser scenario such as Multiple Access for Wiretap Channel (MAC-WTC), Interference Channels with Confidential Message (IC–CM) and Broadcast Channel with Confidential Message (BC–CM). Polar coding schemes for achieving secrecy capacity under strong secrecy constraint for non-degraded wiretap channels is an open challenge and hence, [23], provide a proof for this problem for general wiretap channels by utilizing the Markov chain conditions for securing communication using polar codes. Further, the solution obtained is improved by adding a second layer of encoding and is evaluated for BC–CM. The complexity of encoder and decoder is $O(NlogN)$, where N is the encoding length. Recently, research focus is on hybrid schemes such as polar-AN [24], polar-LDPC [25]. Another promising code is lattice code [26–28]. In [28], theta series of the unimodular lattices generated by Construction A4 from codes over Z4 is calculated by the authors, and a general method to calculate their secrecy advantage is offered. In [29] polar lattices are employed for gaussian wiretap channel model by considering the notion of semantic security. Here, polar lattices which are secrecy good is constructed for gaussian wiretap channel and the authors also prove that it achieves secrecy capacity. Further, the secrecy good polar lattice is applied with gaussian shaping technique which results in an improved secrecy capacity. The complexity involved in encoding and decoding for the scheme considered is $O(NlogNlog(logN))$. Similarly, in [30], the authors proposed an encoder based on lattice coset coding for gaussian wiretap channels in which, secrecy gain is derived for even unimodular lattices. In this encoder, a nested lattice is considered in which, lattice for ensuring reliability at Bob given by Δb and Δe is a sublattice of Bob. Δe increases the confusion at Eve. From the analysis, it is inferred that, with the dimension of lattice, an exponential growth of secrecy gain results. These results are backed by derived examples and asymptotic analysis. Recently convolutional codes [31,32] are also being investigated and explored for enhancing security of wireless networks as it could be a good solution for error correction. By considering the implications of discrete modulations and finite block lengths, in [32], the authors evaluate the levels of PLS that conventional coding schemes can achieve over fading wiretap channels. The average number of attempts needed by an attacker to retrieve the entire message is estimated in real-world scenarios and under outage limitations by focusing on mutual information security. Subject to a certain outage probability, the lower bounds on the wiretapper equivocation is obtained concerning the secret message and evaluate their tightness. The authors also discuss some examples that take into account traditional coding and modulation methods, such as BCH codes and convolutional codes. According to [17], it can be seen that, for the main and eavesdropper channels, authors propose an optimal and practically implementable sub-optimal decoder. Here, convolutional code and its dual is applied to the randomized coding scheme by Wyner to generate a randomized convolutional code of finite length for both gaussian and binary symmetric wiretap channels. Hence, randomized serially concatenated convolutional code is developed. Error probability of codeword is considered as the performance metric. Low security gap is attained with this scheme. 2 provide the advantages, observation and future scope of code based PLS schemes.

2.1.2. Channel adaptation

The idea of channel adaptation to achieve non zero secrecy rate is discussed in literature [33–35]. In this work, we have used the terms channel adaptation and channel variation interchangeably. Independent fading experienced by legitimate link and adversary link can be utilized for our benefit.

Various schemes are proposed in literature. How time domain can be exploited for securing wireless systems is investigated by

Table 2
Comparison of channel code based PLS schemes.

Ref.	Year	Advantages, Observations & Future directions
[17]	2017	Very low security gap <1*dB*, high secrecy capacity without scrambler, practical feasibility and secrecy of the scheme with information theoretic metrics can be analysed.
[18]	2018	Very low security gap <1*dB* with scrambler.
[19]	2015	High performance for small block lengths, practical feasibility can be analysed.
[22]	2016	Better decoding error probability, hence reliable, efficient, practical feasibility can be analysed.
[23]	2016	Strong secrecy under strong security constraints, positive rate shared secret key not required, high decoding probability by Bob, performance of the scheme with a third encoding layer can be analysed, analysis for symmetric wiretap channels can be carried out, practical feasibility can be analysed.
[29]	2018	Achieves semantic security, useful for network information theory applications, integrated approach, semantic security without dithering can be investigated.

authors [36] and here, Hybrid Automatic Repeat Request (HARQ) protocols are evaluated under a secrecy constraint. The authors propose a novel coding scheme called Secrecy Adaptation and Rate Adaptation (SARA) that involves less information leakage and error probability. The proposed scheme has high secrecy throughput. Most of the works for securing wireless communication based on channel adaptation exist for Orthogonal Frequency Division Multiplexing (OFDM) based systems and certain new waveforms such as Orthogonal Time Frequency Space (OTFS), Universal Filtered Multicarrier (UFMC), Generalized Frequency Division Multiplexing (GFDM) are proposed so as to meet certain requirements. However, with the upcoming 5G technologies the need for secure waveform design is essential. Therefore, authors [37] propose secure Orthogonal Transform Division Multiplexing (OTDM) for dispersive channels in which the bases which are orthogonal are extracted from the legitimate users channel. These bases then carry and select data at the legitimate transmitter and receiver respectively. Frequency domain can be utilized for achieving PLS. For e.g. OFDM systems are vulnerable to frequency synchronization. An offset in frequency can highly impact OFDM systems. However, this drawback of OFDM can be used to our advantage. Therefore, authors [38] put forth the idea that controlling the inter-carrier interference as a result of carrier frequency offset in OFDM systems can be really advantageous. In this manner, the adversary channel is degraded without affecting the legitimate links performance, provided the CSI and carrier offset values of the legitimate node are available. BER is the performance metric used.

Authors [39] propose a technique named as Orthogonal Frequency Division Multiplexing with Subcarrier Index Selection (OFDM-SIS) for securing OFDM based waveforms by allowing two security levels, one in FDD and two in TDD. In the proposed scheme, adaptive channel based interleaving converts correlated channel response of the legitimate link to completely uncorrelated ones. The OFDM symbol is further divided into small subblocks. Each of these subblocks contain uncorrelated subcarriers, out of which the good ones are used for transmission of data while all others are suppressed. The technique can be employed for low complexity 5G Ultra Reliable Low Latency Communication (URLLC) services. Exploiting antennas in the spatial domain is an effective way to secure wireless networks. For instance, beamforming technique enables the source to concentrate its energy in the legitimate receiver direction while reducing the energy to the eavesdropper. Therefore, authors [40] develop an array beamforming approach thereby enabling directional modulation (DM) so as to harvest wireless co-channel interference. This approach facilitates independent control of the signal transmitted to the adversary and hence, issues of larger aperture, high sensitivity may not compromise security of the system. By this scheme, the interference can be selectively manipulated without corrupting the desired signal. Since the steering vector formulation is computationally complex, the proposed direction dependent modulation is formulated as a convex optimization problem. Security of Precoded Orthogonal Space Time Block Code (POSTBC) systems is attempted through various techniques of which one technique employs Precoding Matrix Indicator (PMI) as a secret key which is available only between the legitimate parties since PMI information is not shared through any feedback. However, in practical systems such as TDD/FDD, it becomes essential to share PMI via feedback because of possible mismatches in PMI due to channel reciprocity issues which makes a way in for Eve. Even if such a feedback does not exist, through exhaustive search of the codebook, Eve can still make out the PMI. Therefore, to combat this issue, authors [41] propose a scheme by adding the security aspect in POSTBC, that is, precoded OSTBC with partial pre-equalizing for Multiple Input Single Output (MISO) systems. The proposed scheme does not take into account AN as it wastes power resources and key sharing as it can be cracked.

BER is utilized to analyse the security gap. This can be employed for current and future 4G and 5G wireless networks. Interference being a serious issue for all future wireless devices, authors [42] propose schemes to address jamming and eavesdropping attacks in Interference Alignment (IA) based wireless networks. Networks based on IA, align the interference cooperatively into a subspace same as the jamming signal at the receiver using precoding matrix and thus, signal of interest can be decoded without any issue. Further, an AN based scheme in which AN is generated by each IA transmitter disturbs Eve's signals while keeping the legitimate network safe. Next, so as to analyse the likely threat in IA based networks, a scheme termed as Collusive Eavesdropping Scheme (CES) is proposed in which a valid node is eavesdropped with the cooperation of some hostile users. Authors [43] first investigate the efficiency of AN assisted IA technique without WPT and improved it, as there exist AN assisted IA [44] schemes without WPT and issues of power allocation exist in such schemes. Further, without compromising the requirements of information transfer, all the remaining transmit power is assigned to AN for enhancing the anti-eavesdropping performance. Next, an AN assisted IA scheme with Wireless Power Transfer (WPT) is proposed with the aim of fully utilizing the AN and interference among users. In the scheme proposed, the power required for transmitting AN is augmented with the guarantee that the minimum requirement of harvested power and transmission rate is satisfied. Then, closed form solutions for the proposed algorithm is derived for the suboptimal case as deriving the solution for optimal case is computationally tedious as the problem is non convex. Channel can be adapted for enhancing security of wireless networks by utilizing the relays [45] employed. For e.g. the SOP analysis of cognitive radio networks with Cooperative Jamming (CJ) is not focussed much and most of the relay and jammer selection schemes involve much overhead and schemes are impractical when the eavesdropper is passive. Hence, authors [48] propose two opportunistic relay selection schemes with CJ for secure secondary transmission in the presence of concluding eavesdropper whose CSI is unknown. Further, the SOP is derived for each of the schemes. Eavesdropper should not be aware of the relay and jammer selection because, eavesdropper will perform coordinated beamforming to nullify the jamming signal produced and the signal of interest is obtained which can be highly critical for the secrecy of the wireless network.

Therefore, authors [49] propose a scheme to select relay and jammer secretly. Two selection schemes are proposed for Decode and Forward (DF) networks with intermediate nodes used for either communicating with destination or jamming, when multiple passive eavesdroppers are present. In the proposed technique, legitimate destination is aware of the eavesdropper links statistics alone and legitimate links CSI and chooses the relay and jammer such that the SOP is minimized. Further, the legitimate destination broadcasts the information as to which intermediate node acts as jammer or relay while the eavesdropper will not come to know of the selection results. Authors [46] propose to use IRS for enhancing security of the physical layer. In the proposed scheme authors maximize the sum secrecy rate by optimizing the transmit power and phase shift at every element of the IRS. The scheme aims to utilize the IRS and non IRS signals in such a way that they add destructively at the unintended receiver. A sum secrecy gain of about 120 % is achieved by the proposed scheme in comparison with traditional schemes. Authors [47] propose to investigate the PLS performance of Reconfigurable Intelligent Surfaces (RIS) aided NOMA technology for 6G communication systems. So as to enhance the PLS performance, a power allocation strategy and beamforming approach is adopted. Two scenarios are evaluated, one with CSI of eavesdropper and second scenario without the availability of eavesdroppers CSI. It is inferred from the proposed scheme that, when the number of reflecting elements in the RIS is increased, an increase in the secrecy gain is observed. The proposed scheme addresses the dead zone problem in NOMA systems. 3 provides the advantages, observations and future scope of channel adaptation based PLS schemes.

Table 3
Comparison of channel adaptation based PLS schemes.

Ref.	Year	Advantages, Observations & Future directions
[36]	2013	Low security gap, high secrecy, developing the scheme for inputs of finite length can be carried out.
[37]	2017	High secrecy, power efficient, robust, reliable, better BER, high SNR, better than OFDM scheme.
[38]	2016	Good for low power systems, secrecy capacity and channel selectivity can be analysed.
[39]	2017	Good for low power systems, achieves practical secrecy, reliable, low security gap, PAPR can be investigated, impact of various block sizes and out of band leakage can be explored, OFDM-SIS system can be optimized.
[40]	2017	Frequency reuse, efficient information and wireless power transfer, energy efficient and secure, capacity performance evaluation can be done, preserves convexity of the formulation, synchronization effect on power transfer, optimal layout for co-channel information and power transfer and non-uniform array layouts can be explored.
[41]	2016	Power efficient, low security gap with no energy wastage.
[42]	2016	Active attack is investigated.
[43]	2018	Very low computational complexity, algorithm developed is sub-optimal, solution for optimal case can be designed for low computational complexity, efficient power allocation.
[44]	2015	Scheme to enhance secrecy for the challenging situation when the CSI of eavesdropper is unavailable has been effectively analysed, SOP when large number of eavesdropper's are available can be analysed and scheme can be improved to minimise the resulting information leakage.
[45]	2017	Robust against cooperative jamming attack by multiple eavesdropper's, reduced complexity.
[46]	2021	Increases the sum secrecy rate for full duplex system, maximizing secrecy for multi user, multi antenna systems involves future scope
[47]	2021	Improves secrecy performance of the system, increasing reflecting elements contribute to enhanced secrecy performance in contrast to increasing transmit antenna number, trade off between number of reflecting elements and secrecy performance in terms of complexity is not analysed.

2.1.3. Artificial noise

The idea of injecting artificially generated noise [50,51] to make the adversary channel worse is already explored. Adversary's channel condition can be made worse by adding AN, such as jamming or interference, without affecting the legitimate channel thereby ensuring security of the wireless system. In such a scheme, the legitimate user channels null space have certain degree of freedom. With this approach, the perfect secrecy notion may be attained in a non-fading or fading environment. AN can be injected in the temporal, frequency and spatial domains. In time domain, for e.g. authors [52] propose a scheme for securing OFDM systems by employing a transmit filter. In the proposed scheme, the orthogonality at eavesdropper is destroyed, thereby, complicating the eavesdropper's reception while keeping the legitimate communication safe. The residual power available after allocating power for subcarriers is utilized for AN. By this, an AN aided OFDM secure system using transmit filter approach is designed. Another scenario in which AN [53] is introduced in time domain is described next. Introducing AN injection scheme [54] into basic single antenna systems over fading channel is an unaddressed and challenging issue. Therefore, authors propose a scheme to inject AN effectively into single antenna systems. In the system model for the proposed scheme, half duplex receivers are considered and external relays or helpers are absent. Here, effective power allocation and joint rate are also analysed and it is inferred that, by allocating enough power, even perfect secrecy can be achieved. For e.g. AN techniques exploiting spatial degrees of freedom requires that the count of transmit antennas *Ntx* is greater than the count of receiver antennas *Nrx*, by taking into consideration null spaces availability. However, AN techniques exploiting temporal degrees of freedom does not require that $Ntx > Nrx$ because in OFDM systems, AN generation in the temporal domain is by taking advantage of the redundancy extracted from Cyclic Prefix (CP). This scheme is explored only in SISO systems. Therefore, authors [55] explore AN generation in time domain for multiple input multiple output (MIMO)- OFDM systems. In MIMO-OFDM systems, AN generation in temporal domain is possible even if *Ntx* is less than *Nrx* but the number of transmit antenna required is larger or long CP is required. In the scheme proposed, the AN generated in temporal domain is cancelled in the frequency domain and AN can be generated irrespective of length of CP or the number of transmit antennas. Similarly, the frequency domain can also be utilized for enhancing the security of wireless networks. Safe communication in frequency selective channels are explored before also. However, there the necessity of full CSI knowledge of eavesdropper is present. Therefore, authors [56] propose a technique using AN to explore security of frequency selective channels in SISO systems without the need of CSI of eavesdropper. In the proposed technique, subchannels already in fade are excluded and hence reduction in channel capacity of legitimate link is reduced while ensuring that this reduction is proportional to the unused subchannels of eavesdroppers channel capacity. Again, addition of fade filler noise further corrupts the reception of signal at eavesdropper. Here, two cases are analysed, with-AN and without-AN. In without-AN case, there is high chance of attaining non zero secrecy capacity by using sub-channels of legitimate node. With-AN case completely disturbs the adversaries reception with an error floor, for high SNR regime. The spatial domain can be exploited to the benefit of securing wireless systems by manipulating the antenna and relay elements. For e.g. [50,51,57,58] in the case of antenna, when eavesdropper has CSI information and enough number of antennas, it is always possible for eavesdropper to have better channel than legitimate receiver. When Eve has no CSI, then schemes such as randomized beamforming transmission scheme helps in forfeiting Eve's attempt to perform blind deconvolution to obtain CSI. However, by this scheme Eve's BER is 0.5 but secrecy analysis is not done. Again, in a later work, secrecy analysis is performed but for Eve with single antenna. However, the lower bound of secrecy rate achieved is loose and robustness of the scheme to multi antenna eavesdropper is not investigated. Therefore, authors [59] re-investigate randomized beamforming scheme for the scenario in which passive adversary is outfitted with multiple antenna (MISO channel) and explore the secrecy rate. In the proposed scheme, Eve has fast fading channel and hence it is called artificial fast fading (AFF) scheme. Eve experiences a non-coherent rician fading SIMO channel. Two schemes such as AN and AFF are compared. Expression for single antenna Eve is derived, further, a lower bound for multi-antenna Eve is also derived. To investigate power allocation problem, a hybrid AFF-AN scheme is proposed and achieves better secrecy performance. Randomized beamforming is another technique by which AN can be injected. Transmit Beamforming (TBF) schemes have two issues, one is the count of radio frequency chains linked to every antenna and the signal processing required is very high. Second, an Eve employing blind equalization technique can easily detect the confidential information and violate the secure communication. Therefore, authors propose [60] a Generalized Selection Transmission (GST) technique with Randomized Beamforming (RBF) is proposed, with the aim of addressing both the problems of TBF. In the proposed GST scheme, signal processing and power usage is reduced to a reasonable level by choosing a subgroup of transmit antennas having very strong fading channel gains. Further, closed form expressions for exact and asymptotic SOPs with RBF/GST as well as GST is derived for passive eavesdropping case in which, the eavesdroppers statistical CSI is available at the transmitter. It can be inferred that the same secrecy outage diversity gain is achieved by GST as TBF in MISO wiretap channel. For active eavesdropping case, in which perfect CSI of adversary is known at the transmitter, expression for ergodic secrecy rate of GST and RBF/GST is derived. It is inferred that RBF/GST performs better than GST in terms of ergodic secrecy rate performance and provides enhanced security in MISO wiretap channels. It is also inferred that when the number of antenna is reduced to a particular level, the RBF/GST secrecy is not affected considerably. Relay [61] can be exploited for injecting AN to the adversarial channel. For e.g. security in Cyber Physical Systems (CPS) is critical and essential due to certain reasons and applying PLS schemes in CPS might face several new issues such as, multi relay aided coordinated transmission. Most of the CPS physical elements are managed in a distributed manner, simpler design of transmission protocols could be considered otherwise it will be inapplicable as complex control messages are involved. Next is deploying multi antenna techniques which has proved its capability to adequately control the signal beam direction and manage interference among users effectively becomes highly expensive when it comes to CPS as extensive deployment of multi-antenna devices are needed. Therefore, authors [62] consider SISO with a preselected relay to forward the message which employs amplify and forward protocol. The relay is placed because of the absence of direct source to destination link. So as to reduce the complexity a Maximal Ratio Combining (MRC) receiver is opted which has less complexity than Minimum Mean Square Error (MMSE) receiver. In the proposed AN-AF scheme, forwarding of source message by relay and injection of AN happens concurrently. Here, first, perfect eavesdropper CSI is considered and the AF coefficient for forwarding the information signal and AN covariance are optimized for attaining the maximum attainable secrecy rate. Optimum result is obtained by using 1D search and solving a sequence of SDP's. In the next scenario, eavesdropper CSI with channel estimation error is analysed and the achievable secrecy rate's lower bound is also obtained. A combination of DM and AN is proposed by authors [63] to enhance PLS of wireless networks. The proposed scheme also involves intelligent reflecting surfaces to aid the scheme. The proposed scheme is evaluated in terms of secrecy rate and SNR. The scheme outperforms most of the existing and conventional approaches thereby proving as suitable for PLS. The security of UAV networks with the enabling technologies such as NOMA and mmWave communications is investigated by authors [64]. The malicious users degrade the performance of UAV networks, therefore, the authors propose to employ a transmission strategy based on NOMA in mmWave networks. In this work a protected zone is developed to ensure security of the wireless networks. The performance is evaluated in terms of size of the protected zone, power of transmission and altitude of the UAV on secrecy performance. 4 provide the advantages, observations and future scope of AN based PLS schemes. 3 illustrates the most common performance metrics employed to evaluate the performance of key less PLS schemes.

Table 4
Features of AN based PLS schemes.

Ref.	Year	Advantages, Observations & Future directions
[50]	2005	Improved secrecy performance for OFDM systems, AN injection does not disturb Bob, errorless transmission for Bob even at $10dB$ SNR.
[52]	2016	Possibility to achieve perfect secrecy, AN scheme can be extended to multi-antenna systems.
[53]	2016	Increased scalability of AN without compromising secrecy rate.
[54]	2017	High secrecy without knowledge of CSI.
[55]	2014	Scheme can be evaluated for large scale fading scenario.
[56]	2014	Improved secrecy with fair signal processing and power utilization.
[60]	2018	Better secrecy rate, scheme can be investigated for scenarios having severe path loss by optimizing transmit power such that impact of AN on legitimate user can be minimized and secrecy rate can be enhanced.
[63]	2020	Increasing reflecting elements increases the secrecy performance, renders 2D secure transmission, trade off between number of reflecting elements and secrecy performance in terms of complexity is not analysed.
[64]	2018	Provides superior performance in contrast to OMA

2.2. Approaches to enhance key less PLS

Here, two highly relevant options to enhance key less PLS i.e. IRS and AI is explored. We have summarized few works that discuss the various means of exploiting these concepts. IRS technology improves the wireless data transmission system performance by employing small reflecting units in large numbers that are adjusted jointly so as to redesign the wireless signal transmission environment. Another key concept that has already become the driving force of various emerging technologies like IoT, big data, robotics to name a few, is AI. In simple terms, AI is the ability of computer systems to carry out processes associated with human intelligence.

2.2.1. Intelligent reflecting surface and Physical layer security

Here, we present a discussion on another emerging, interesting and vividly researched area i.e. IRS [65,66]. In [67] authors propose a point to point IoT system aided with RIS. To explore the feasibility of RIS aided IoT system, the authors consider closed form expressions of secrecy capacity and secure outage probability metrics with the aim of arriving at those system parameters that facilitate performance improvement of RIS aided IoT system. With respect to the number of metasurface elements, through an extensive mathematical analysis, the authors explain the relevance of RIS configuration as well. The results show that more number of reflecting elements provide better security output. IRS for improving the secrecy performance of wireless downlink communication is discussed by authors in [68] by proposing an algorithm that jointly optimize the passive and active beamforming when the

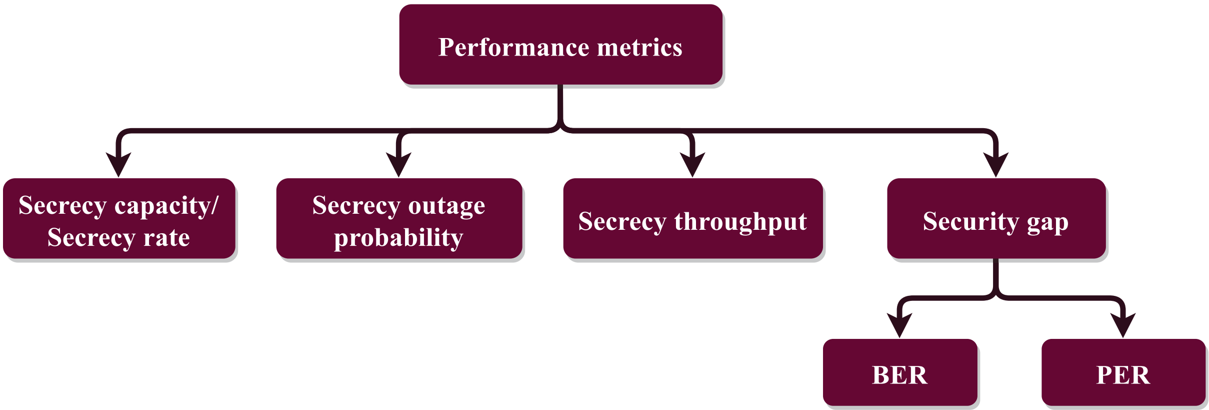

Fig. 3. Common performance metrics to evaluate key less PLS.

legitimate node is equipped with a single antenna while the eavesdropper has a mutli antenna system. The algorithm aims at optimizing the IRS phase shift via Fractional Programming (FP) and Manifold Optimization (MO), both of which are of low complexity. The scheme renders a near optimal phase shift for IRS. Besides this, the authors also derive the beamforming vector at Base Station (BS) that is optimal for fixed phase shifts for IRS. In [69], the authors explore the performance of IRS aided NOMA networks specifically downlink communication in the presence of an eavesdropper, in terms of SOP and Average Secrecy Capacity (ASC). In this work, the quality enhancement upon employing IRS for assisting the communication between cell edge node and BS is investigated. The performance evaluation is performed by considering a Nakagami-*m* fading channel in terms of fading parameter and the number of IRS elements. At 30 dB transmit SNR, the SOP is 10^0. The ASC increases with transmit SNR, at 60 dB transmit SNR, the ASC is in the range of 2 Mbps. The SOP seems to decrease with the number of IRS elements. In [70], authors propose a novel scheme that involves channel randomization using RIS. The scheme is employed in a TDD downlink cellular system with one BS equipped with multiple antennas, multiple RIS elements, multiple users and multiple eavesdroppers. The authors also assume that only LoS exists due to tera hertz spectrum that might be employed in 6G wireless communication. In the proposed scheme, reflection matrices are pseudo randomly generated by each RIS initially. Then this is employed for pilot signal duration and data transmission duration in the uplink and downlink respectively. Further, estimation of wireless channel of user devices with all RIS reflection matrices is performed by the BS and the user equipment with the best secrecy rate for every reflection matrix is chosen. By the proposed method, secrecy rate of $>$4bps/Hz is achieved at 15 dB transmit SNR. Upto 20 users, the secrecy rate achieved is $>$4 bps/Hz. When the number of RIS elements is 16, again the scheme can achieve a secrecy rate of $>$4bps/Hz.

Again, in [71] authors explore the benefit of employing RIS for downlink transmission, when the users are randomly located and when the eavesdropper is equipped with multiple antenna. Here also, the performance of the system is evaluated in terms of SOP, average secrecy rate and probability of non-zero secrecy capacity. The authors derive exact probability density function and cumulative distribution function of the received SINR via stochastic geometry theory. From the investigation it is inferred that, for higher number of reflecting elements, performance of the system is better in contrast with the case when less number of elements are considered especially when the path loss associated with NLoS is less. The RIS aided system performs much better than Non-RIS aided system. In [72], authors propose a novel RIS design for improving PLS in NOMA systems by removing the signals received at the eavesdropper end especially when the channel gain of legitimate user is less than that of Eve. In most of the existing works, secrecy performance of the legitimate user is enhanced by designing RIS. However, in this work it is different. The special outage probability is evaluated for varying transmit power. The proposed NOMA network with RIS aided design renders superior performance than conventional NOMA networks. In [73], authors investigate PLS in IRS assisted networks in which, the transmitter sends information to multiple IoT devices via energy collected from power station. Here, it is assumed that the communication takes place in the vicinity of multiple eavesdroppers. The authors propose to employ a stackelberg game approach to secure systems. The IRS assisting facilitate efficient energy transfer as well as safe information transfer. The scheme involves trading of energy between the transmitter and power station, both of which belongs to distinct service providers. In this trading, the transmitter pay an incentive to the power station for the energy assistance. The mentioned inter activity is modelled via the proposed game approach. The non-convex problem is resolved by decomposing it into subproblems. Alternating Optimization (AO) and semi-definite relaxation methods are employed to solve the subproblems. The approach has been compared with existing schemes that does not employ IRS and it is inferred that, the proposed approach render better results in terms of the time taken for transferring energy wirelessly and utility of transmitter and power station. Due to a greater bandwidth, higher data rate, and more efficiency, Visible Light Communication (VLC) is one of the most promising supporting technologies for future 6G networks to overcome radio frequency based communication restrictions. VLCs, on the other hand, are vulnerable to all known wireless communication security vulnerabilities (e.g., eavesdropping and integrity attacks). As a result, security experts are proposing novel PLS solutions to safeguard such communication. Among the various solutions, current work has successfully demonstrated the innovative RIS technology linked with VLCs to boost VLC communication capacity. However, there is still a paucity of analyses and solutions in the literature to demonstrate the PLS capability of RIS-based VLC communication. In this research, Watermark Blind Physical Layer Security technique is employed to protect VLC communication at the physical layer by combining watermarking and jamming primitives. The proposed scheme in [74] makes use of RIS technology to improve the communication's security features. RIS phases are generated to maximise the jamming interference pattern over a predetermined area in the room using an optimization framework. In particular, the proposed technique outperforms a scenario without RIS in terms of secrecy capacity without making any assumptions about the intruder location.

The good impact of an RIS-assisted solution on the legit jamming receiver's secrecy capability in a VLC indoor scenario is verified. It can be inferred that, RIS technology expands the region where secure communication can take place and that, increasing the number of RIS material reduces the likelihood of an outage. To quantify the secrecy performance of NOMA-RIS-aided IoT systems, the authors, in [75], focus on secure performance parameters at the legitimate users, such as SOP and secrecy capacity. It is assumed that, the RIS is located between the access point and the legit devices, and that, the smart phase shift mechanism of metasurface elements in the RIS will improve security of the link. The SOP and secrecy capacity analysis is presented. The optimum SOP is then presented using an iterative search technique for further information and insights. To achieve secure performance, an efficient Deep-Neural Network (DNN)-based secure metric prediction scheme is used to assist the BS in effectively allocating power coefficients to NOMA users. It is inferred that, the number of RIS metasurface elements and the average SNR at the BS have the greatest impact on system performance.

2.2.2. Artificial intelligence and Physical layer security

AI will be a key factor in 5G/6G infrastructure and hence, another interesting development in PLS is the involvement of AI [76,77]. Therefore, next we discuss some of the recent works that explore this combination. Eventhough many schemes have been proposed and developed for enhancing PLS, when it comes to deploying practically, key less or SINR based PLS schemes face challenges such as lack of knowledge of eavesdropper's CSI. In most of the SINR based approaches developed, it is assumed that, we have CSI of eavesdropper pre-acquired and has full knowledge. However, eavesdropper can be distributed as well, when it comes to practical scenarios. Similarly, another issue is in the assumption of channel model and network model. Most of the PLS schemes developed are for point to point models and with very little inclusion of Heterogeneous Networks (HetNets) as well as multiuser environments. It is required to investigate more on PLS in massive MIMO and Millimeter Wave communication (mmWave) channel models as most of the investigation is on parallel Rayleigh or Gaussian channel models. Therefore, in [78], authors develop a framework of adaptive secure resource management based on active cognition in which, rather than inputting the specific eavesdropper, the distribution of eavesdropper is learnt by the network operator actively. The authors explore the potential of AI and edge computing in facilitating PLS practically. Next, to establish D2D pair optimally and to effectively select transmit antenna in cellular networks, the authors develop a framework based on Deep Learning (DL) for enhancing PLS in [79]. The proposed schemes namely, long short term memory and echo state network ensures secure communication while accessing the next time slot to determine the antenna selection which become insecure due to user mobility. The proposed scheme even increase the BS life as well. In [80], authors employ the concepts of DL to ensure security of the physical layer. The proposed scheme employs neural networks and develop an authentication scheme for the physical layer by developing an intelligent authentication scheme that learns the data characteristics. This is developed for the data collection unit. The development of an AI-based methodology for extracting authentication features that casts the authenticator to the blind learning space of the feature is carried out. It does not require a channel variation pattern. Based on test results and adjustable factors at the physical layer, the learning-enabled authentication process is thus seen as a classification system that is simpler to train. For Simultaneous Wireless Information and Power Transfer (SWIPT) systems with a power splitting scheme, the authors in [81], consider an IRS-assisted safe transmission maximisation technique. In order to meet the needs of energy harvesting at the user and transmit power at the transmitter, first the authors seek to maximise the secrecy rate of the system by determining the ideal transmitter power, user equipment, power splitting factor, and IRS phase shifts. An AO approach is utilised to solve the optimization problem, which alternates between using the feasible point pursuit–successive convex approximation iterative process and the penalty method to obtain the best solutions. It can be inferred that, in comparison to the non-IRS scheme, the method assisted by the IRS achieves a significant improvement in terms of average secrecy rate.

In Fig. 4, the techniques under channel coding, channel adaptation and AN approaches are provided where $CV - SA$ denotes channel variation in spatial domain using antenna, $CV - SR$ denotes channel variation in spatial domain using relays, $CV - T$ denotes channel variation in time domain, $CV - F$ denotes channel variation in frequency domain, IA denotes interference alignment. Similarly, $AN - T$ denotes AN in time domain, $AN - F$ denotes AN in frequency domain, $AN - Antenna$ denotes AN in spatial domain using antenna, $AN - Relay$ denotes AN in spatial domain using relays, and RB denotes randomized beamforming in spatial domain.

3. Application of PLS in IoT

IoT [82–87] in which, all physical objects made of sensors and softwares for enabling connectivity are connected, is going to be the next future. 5 illustrates the various promising application scenarios of IoT. With the fast growth of wireless technologies such as 5G, 6G, the demand for information sharing and access, the time sensitive applications such as tele-surgery to name a few are exploding. It is envisioned that the connections will increase to 28.5 billion and the mobile data traffic could reach 2.5 exabytes per day by 2022 when analysed globally [88]. Obviously, security issues are also going to be high. It is extremely essential to develop schemes to ensure security of the physical layer. As IoT's are low power devices, security schemes must also ensure not to take up a lot of energy of the device. Therefore, schemes having low complexity and with optimal energy utilization is a hot area of research when it comes to IoT. This motivated us to explore the current developments in terms of security in this area.

Communication systems which are URLLC are one class of service which next generation wireless system aims for. It is envisioned that, URLLC systems will be having an ultra high reliability with an error probability of 10^{-7} and end to end latency of $1ms$ [89]. There are immense new opportunities with the onset of URLLC systems such as tele-surgery which are all time critical applications, 5G tactile internet etc. Enhancing the security of such networks is really challenging also. As PLS schemes are less complex and with a lot of advantages suitable for dynamic wireless systems in contrast to the traditional cryptography, authors [90] explore the PLS schemes and performance metrics suitable for URLLC systems along with a comparison of the tradeoff between reliability, security and latency. Through the analysis, it is inferred that, among the various information theoretic performance metrics such as, perfect secrecy, weak secrecy, strong secrecy, secrecy capacity, SOP, only perfect secrecy is applicable in URLLC while error rate such as security gap and rate interval are applicable in URLLC systems. To summarize, PLS is the potential solution to enhance security in the context of URLLC due to its low complexity. Among performance metrics security gap and rate interval are applicable to analyse URLLC system in terms of security. Location based beamforming might be helpful to ensure security of certain URLLC scenarios with Line of Sight (LOS) components available. Authors [91] develop a scheme in which, the secrecy performance is enhanced by developing a probabilistically robust and hybrid

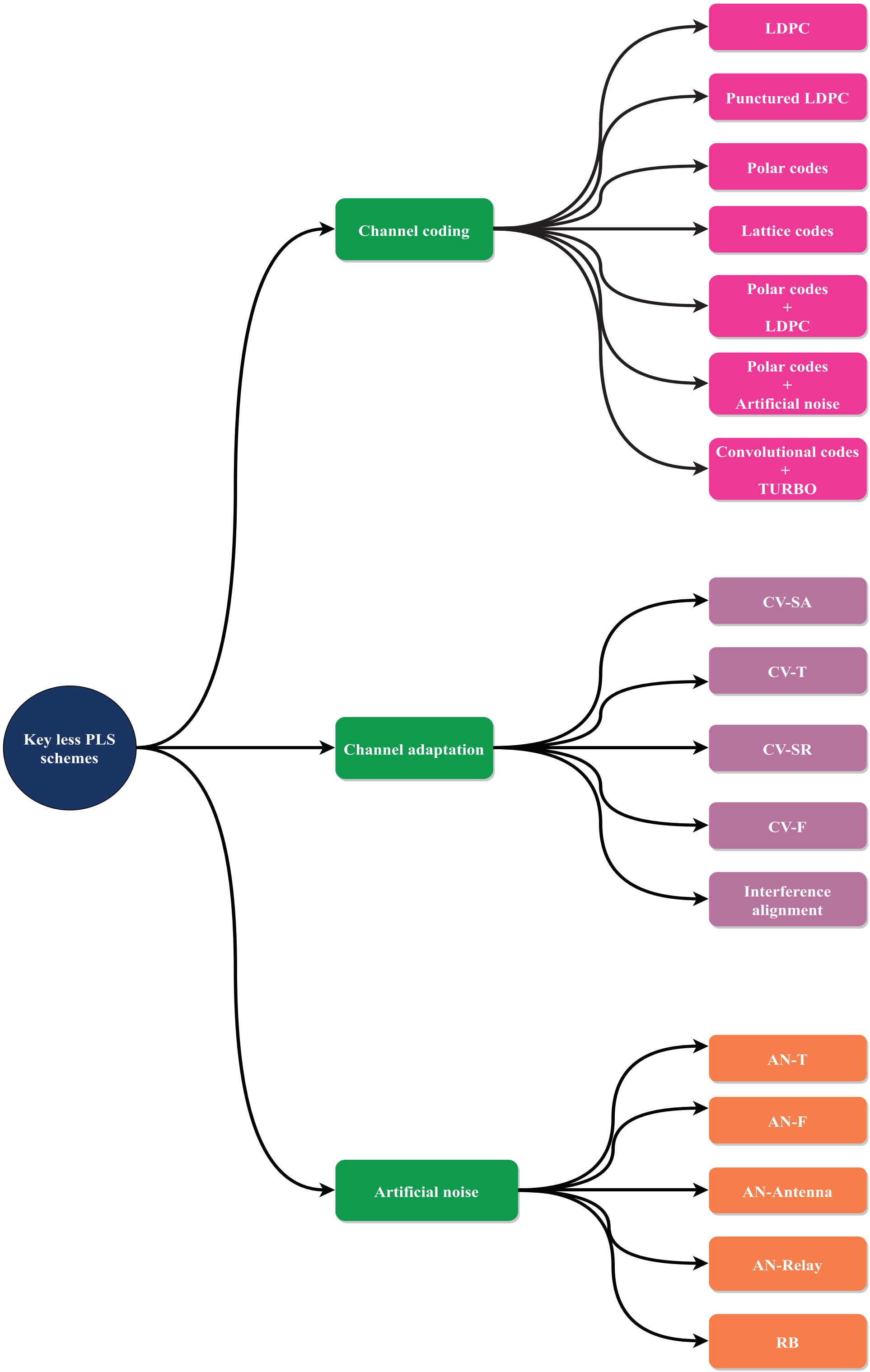

Fig. 4. Channel code, channel adaptation and AN based schemes.

precoding scheme which is not sensitive to the adversary's imperfect CSI. The precoding strategy is usually adopted for mmWave communication networks due to its excellent tradeoff between hardware complexity and spectrum efficiency. In this work, both digital and analog precoders are designed for maximizing the low secrecy rate of IoT devices in terms of secrecy outage constraint and information rate of every IoT device when a Gaussian CSI error model is considered. In [92], the authors propose a space shift keying scheme to enhance secrecy of IoT devices by using antenna selection and AN injection. In the proposed scheme, antenna selection is performed with respect to the signal to leakage noise ratio and AN degrades the channel of Eve while cancelling the interference at the legitimate link. The proposed scheme is evaluated in terms of bit error ratio and secrecy rate. For the proposed scheme,

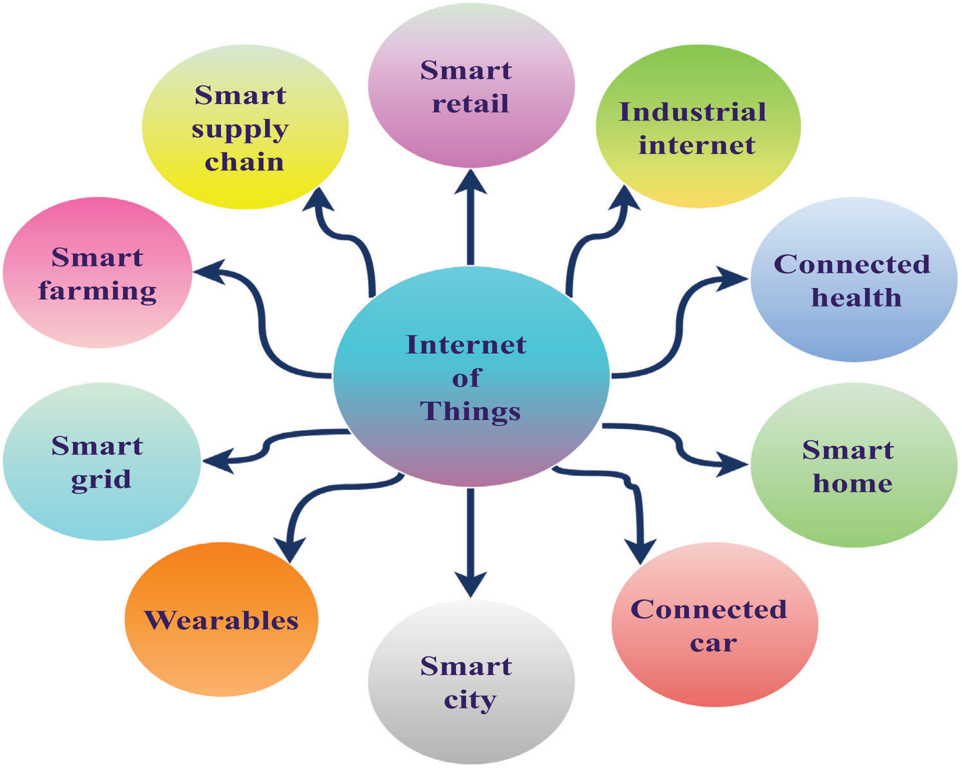

Fig. 5. IoT application scenario.

a secrecy rate of > 2 b/s/Hz and BER $< 10^{-1}$ is achieved at an SNR of 15 dB. However, the authors have not discussed how AN is effective in low power devices in an IoT environment. In terms of system complexity, the overhead at the transmitter side and complexity of detection is reduced as SSK [93] scheme which is simplified variant of spatial modulation is employed.

Authors [94] propose a novel scheme considering few cutting edge technologies for developing a secure and high data system for 5G centric sensor enabled IoT systems. The benefits of Virtual MIMO (V-MIMO), SWIPT and beamforming are utilized to develop the framework. Further, by employing an iterative algorithm with penalty functions, the secrecy rate maximization problem is solved. The performance of the proposed framework is evaluated using energy efficiency, total energy harvested and secrecy rate. In DM, the main idea is to amplify the signal power in a particular desired direction by using a known modulation scheme while scrambling the signal in other directions. In DM scheme, there is a very high complexity involved when using analog circuits due to the complex number format of the weight coefficient for each transmit antenna in the array is a complex number which when processed by analog circuits results in different magnitude and phase responses for the feed circuits. To address this, authors [95] propose to use a constant magnitude and hence, only phase control is performed for the DM scheme. Due to the low complexity, power consumption and secure design, the proposed scheme is suitable for 6G enabled IoT devices. Cognitive Ambient Backscatter Communication technology (C-AmBC), is considered as the driving and one of the most promising technology for green IoT devices. When it comes to employing 5G and 6G communication networks for the massive green IoT, challenges such as optimal energy consumption comes into picture in the context of global warming. In contrast to conventional backscatter devices, omnipresent ambient radio frequency signals are used for enabling communication by just modulating and reflecting the signals to the backscatter device instead of sinusoidal carrier signals having high power. However, due to this simple transmission strategy, C-AmBC technology is exposed to various security threats. Therefore, authors [96] investigate the performance of C-AmBC networks in the presence of unlicensed eavesdropper by proposing a novel framework combining ambient backscatter communication and cognitive radio technology and evaluating the outage and intercept probabilities. The communication of wireless sensor nodes is highly challenging in the smart city application of IoT. Therefore, in [97], authors investigate the secrecy performance of the mobile wireless sensor communication network in smart cities by deriving the closed form expressions of SOP and strictly positive secrecy capacity of two transmit antenna systems over 2-Nakagami fading channels. Smart energy systems are an integral part for realizing the smart city vision. To achieve smart energy systems, numerous computing and communication techniques are considered which increases the vulnerabilities at all layers. Therefore, in [98], authors discuss the physical layer vulnerabilities in smart grids, the details of which are presented in 6 and also developed a framework (a general model that includes schemes that we have mentioned already such as AN) for securing the physical layer in smart grids. Now, to combat these vulnerabilities in smart grids, some solutions such as detecting anomaly by comparing healthy behaviour of the system with pre-analyzed observations of system behaviour and spread spectrum techniques that come with intrinsic anti-interception and jamming properties can considerably improve the secrecy performance here. The fourth industrial revolution termed as ‘Industry 4.0’ which involves employing smart technology to automate conventional techniques and practices. On employing smart technology in the agricultural domain, it is termed as, Agriculture 4.0, smart agriculture or smart farming. PLS schemes can be employed to secure agricultural sector from various vulnerabilities as discussed in [99–103] to enable secure smart farming. Intelligent Transportation System (ITS) is really helpful as it renders efficient

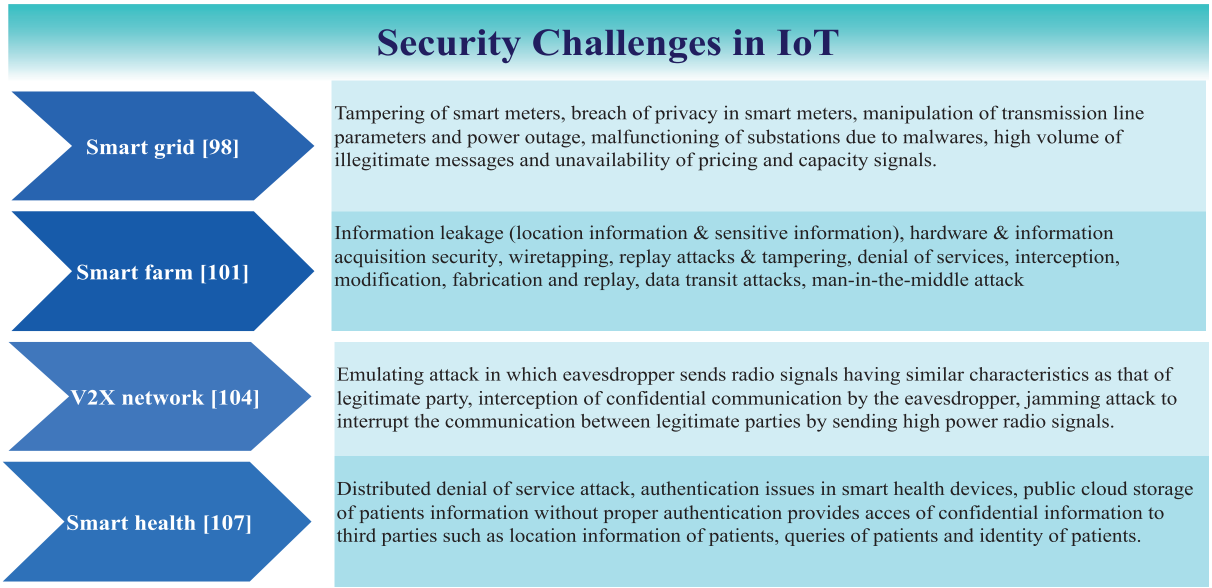
Security Challenges in IoT
Smart grid [98]
Tampering of smart meters, breach of privacy in smart meters, manipulation of transmission line parameters and power outage, malfunctioning of substations due to malwares, high volume of illegitimate messages and unavailability of pricing and capacity signals.
Smart farm [101]
Information leakage (location information & sensitive information), hardware & information acquisition security, wiretapping, replay attacks & tampering, denial of services, interception, modification, fabrication and replay, data transit attacks, man-in-the-middle attack
V2X network [104]
Emulating attack in which eavesdropper sends radio signals having similar characteristics as that of legitimate party, interception of confidential communication by the eavesdropper, jamming attack to interrupt the communication between legitimate parties by sending high power radio signals.
Smart health [107]
Distributed denial of service attack, authentication issues in smart health devices, public cloud storage of patients information without proper authentication provides acces of confidential information to third parties such as location information of patients, queries of patients and identity of patients.

Fig. 6. Security challenges in Industry 4.0.

traffic management, reduced accidents and thereby improved safety due to the inter-vehicular, intra-vehicular and vehicle to infrastructure communications. However, securing the physical layer is of utmost importance in Vehicle to Everything (V2X) networks as well. Therefore, in [104], authors devise schemes to ensure security of V2X networks. In [104], the authors mention that, to improve PLS in V2X environment, relaying is advantageous, especially, when there is a lack of direct link that is reliable. Another case where relaying helps is when the Vehicle Penetration Loss (VPL) is considered. According to [105], due to VPL, the signal attenuation can be as high as 25 dB at various frequencies. This can be resolved using moving relays that are equipped with both an indoor and outdoor antenna. In [106], authors employ an IRS aided vehicular network. Two scenarios are considered, one uses vehicle-to-vehicle communication with an RIS-based access point as the source, while the other uses a Vehicular Adhoc Network (VANET) with an RIS-based relay on a building as the source. To explore the average secrecy capability of the considered systems, both models assume the presence of an eavesdropper. It is inferred that, with source transmit power and number of RIS elements, the ASC increases (> 0.6). Another emerging area is smart health systems, wearable devices form an integral part of smart health system and it is highly scalable because of which a lot of security vulnerabilities arise [107]. As a solution to passive eavesdropping events while transmitting electroencephalogram measurements, an optimization problem has been developed by the authors in [107], that ensures energy efficient transmission and low signal degradation. The proposed scheme works well at all channel conditions and outperforms existing schemes. One of the main performance metric employed here is SOP. Similarly, in the supply chain [97,108] system also a lot of security challenges exist. As a solution for enhancing security in the supply chain and retail sector, in [109], authors develop a security framework for smart supply chain and retail wherein the authors present a novel method for gathering backscatter information from a chipless RFID tag. In order to detect clone or fake tags in commercial applications, a DL model is employed. The proposed method demonstrated a throughput of 99 percent, a favourable and compelling result which suggests that, the technology may be a low-cost solution to the problems. As of now, for IoT security, among the three approaches discussed in this manuscript i.e. channel code, channel adaptation and AN, the more preferred approach is AN, wherein an interfering signal is injected into the desired receivers null space with the aim of degrading the SNR of the adversarial receiver. By this approach, perfect secrecy can be achieved and can also be applied when the adversary is more close to the BS in contrast to other users. The AN based approach has only moderate CSI requirements and the computational complexity involved is only moderate which makes it a potential and promising approach for IoT security. Though injecting AN is a successful method to enhance the link quality of the legitimate node, as most of the AN based PLS schemes deploy multiple antennas at the transmitter and has low energy efficiency, which pose a challenge in its full-fledged consideration for IoT devices, research in AN approach for key less PLS is directed towards improving this aspect. One such scheme is cooperative AN injection [110–112]. Also, AN schemes can be integrated with various other schemes [113,114] to enhance the system security performance further. Next preferred among the three could be channel adaptation approach that is based on space time coding concept i.e. from a matrix codebook, one best precoding matrix is selected so that the SNR at the legitimate receiver is maximized. This approach also requires moderate CSI and also has high energy efficiency. However, the approach has high complexity and cannot promise perfect secrecy for every channel condition of the adversary. The next choice would be channel code based approach, the assumption in channel code based approach i.e. the channel conditions of Eve is degraded than the legitimate receiver is practically tough to realize because it is extremely difficult to obtain the CSI information or location of an adversary who is not present within the network or of passive type.

To summarize, the growth of technology is happening at a lightening speed with a multitude of highly promising applications for a better tomorrow. However, securing such systems is highly essential as there exist a lot of security challenges which need to be addressed as discussed before. 6 summarizes some of the security challenges in IoT.

4. Open research challenges & future directions

Various key less PLS schemes are available and is researched vividly. Now an emerging area in PLS is cross layer PLS [115]. Various key less and key based approaches to tackle the passive eavesdropper exist in literature. Passive attacks include interception and traffic analysis. However, key less approaches to secure wireless networks from active attacks are sparse. Active attacks are accomplished via contamination, spoofing and jamming. To be specific, pilot contamination, feedback contamination, identity spoofing, sybil attacks, pilot jamming, proactive jamming and reactive jamming. Active attacks will be prominent in future wireless networks and it is possible that, for jamming, the adversary might employ multiple antennas and thus, the intensity of jamming will be high. Therefore, so as to implement anti-jamming scheme, legitimate users too will increase the number of antennas, thereby a gush in CSI overhead and complexity occurs. Hence, so as to counteract jamming in the presence of active jammers, systems with fewer antennas is essential. AN schemes are highly effective when it comes to reducing eavesdropping effect at the same time protecting legitimate network. However, when multiple sub-networks exist, inter-cluster interference caused by AN schemes could be huge and tackling this issue with fewer number of antennas is a big challenge. The issue of eavesdropping within wireless networks based on IA schemes in the presence of hostile wiretapper is another big challenge. Most of the schemes employed for enhancing security in wireless networks are complex, therefore, diverting attention to stochastic geometry concepts by learning distribution of jammers and eavesdroppers might help in developing less complex algorithms. Due to the extra low latency requirement of URLLC systems, it is infeasible to obtain accurate CSI. Non coherent communications which does not involve CSI can be employed in URLLC systems due to its low latency requirement. However, reliability will be reduced. Hence, solutions to tackle this challenge is essential. Designing efficient feedback strategy is another challenge in URLLC systems. In V2X communication networks, commonly employed channel models do not fit in when it comes to evaluating performance of the network. Apart from this, hand off issues due to high mobility in such networks is also an open challenge. PLS schemes that take into account the issues with upcoming applications such as delay-sensitivity, stringent processing requirements and low power are very less and hence, considering the Quality of Service (QoS) requirement PLS schemes are to be designed. Practically, to achieve security, it is necessary to develop schemes that have higher QoS than that of Eve. An optimal design is yet to be developed for key less PLS which satisfies all these. Any signal processing needed other than standard communication should be regarded an added load on many low-cost IoT devices due to limited hardware, low complexity, and severe energy limitations. A good PLS solution should not necessitate any changes to the low-cost IoT devices or add any additional processing or communication overhead. As a result, several existing processes, such as sophisticated pilot design and retransmission, cannot be claimed to be optimum solutions. However, we may allow some additional signal processing or computing at BS, which often has more resources and power. Therefore, as existing methodologies in wireless 5G/6G IoT systems do not take into account the low complexity profile, future designs should consider this. Due to superposition of data and AN subspaces, PAPR increases in AN based schemes. This is an open research challenge in AN based schemes. Mobility and security is an area that can be explored. Mobility will be an inherent attribute in upcoming IoT applications such as UAV, smart transportation [116] among many others. Both the legitimate and attacker may be involved. Legitimate party may move to a location to prevent attack while attacker might choose a location to launch an attack. What could be the impact of mobility on attacks that challenge the physical layer is an open area of research. PLS schemes are still not researched vividly when it comes to all the upcoming applications such as IoT, 5G-Tactile Internet, vehicular communication, massive machine-type communication, remote surgery among many others. PLS schemes that take into account the issues with upcoming applications such as delay-sensitivity, stringent processing requirements and low power are very less and hence, as mentioned before, considering the QoS requirement PLS schemes are to be designed. Practically, to achieve security it is necessary to develop schemes that have higher QoS than that of Eve. Deep deterministic policy-gradient algorithms and deep Q networks in deep reinforcement learning are viable ways to overcome the issues associated with meeting the real-time processing needs of large-scale heterogeneous communication systems. The combination of UAVs and IRS opens intriguing research areas due to the advantages of UAVs in considerably enhancing capacity, throughput, and dependability. The location and trajectory of the UAV are two new aspects that present particular difficulties, as do channel modelling and estimate. Cognitive Security (CS) [117,118] is another emerging area to secure digital and physical systems where the channel and environment is first detected and information about the scenario is collected and combined which is then employed for ensuring security by adapting the different propagation attributes to secure the system.

5. Conclusion

With the rapid growth of wireless networking, the need to secure information has become extremely crucial and key less PLS is one promising approach to ensure the desired security due to various advantages such as low complexity, no need of key management infrastructure, solves key distribution problem and is considered to be highly suitable for the low power devices and dynamic modern communication technologies, in contrast to traditional cryptography which involves a lot of practical hurdles. In this paper, we have provided a proper classification of wireless network security. Further, we have classified the key less PLS schemes on the basis of SINR as channel coding, channel adaptation and AN schemes. Next, we have carried out a systematic investigation of the various recent key less PLS schemes employed in literature. We have provided the advantages, observations and future directions for each of the techniques. PLS is an interesting area to research due to its relevance in various upcoming applications such as IoT, 5G-Tactile Internet, vehicular communication, mMTC, remote surgery, BAN among many others. We anticipate the need for security in IoT as it is a rapidly growing domain with a variety of application scenarios. As a result, we have included a summary of the different recent research that examine the potential for key less PLS in IoT. Further, a description of other emerging areas in the context of key less PLS such as AI in PLS and IRS for PLS are also presented. To aid the readers in research in this domain, we have also provided the open research challenges and future directions in key less PLS along with a summary of some of the existing security challenges and solutions in various application scenarios of IoT.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgment

The authors would like to thank the editors and anonymous reviewers for providing insightful suggestions and comments to improve the quality of research paper.

References

[1] C.T. Zenger, M. Pietersz, J. Zimmer, J.-F. Posielek, T. Lenze, C. Paar, Authenticated key establishment for low-resource devices exploiting correlated random channels, Comput. Netw. 109 (2016) 105–123.
[2] K.S. McCurley, The discrete logarithm problem, in: Proc. of Symp. in Applied Math, Vol. 42, USA, 1990, pp. 49–74.
[3] C.H. Bennett, G. Brassard, Experimental quantum cryptography: the dawn of a new era for quantum cryptography: the experimental prototype is working, ACM Sigact News 20 (4) (1989) 78–80.
[4] Y.-S. Shiu, S.Y. Chang, H.-C. Wu, S.C.-H. Huang, H.-H. Chen, Physical layer security in wireless networks: A tutorial, IEEE Wireless Commun. 18 (2) (2011) 66–74.
[5] A. Mukherjee, S.A.A. Fakoorian, J. Huang, A.L. Swindlehurst, Principles of physical layer security in multiuser wireless networks: A survey, IEEE Commun. Surveys Tutor. 16 (3) (2014) 1550–1573.
[6] Y. Liu, H.-H. Chen, L. Wang, Physical layer security for next generation wireless networks: Theories, technologies, and challenges, IEEE Commun. Surveys Tutor. 19 (1) (2016) 347–376.
[7] C.E. Shannon, Communication theory of secrecy systems, The Bell Syst. Tech. J. 28 (4) (1949) 656–715.
[8] A.D. Wyner, The wire-tap channel, Bell Syst. Tech. J. 54 (8) (1975) 1355–1387.
[9] J. Zhang, T.Q. Duong, A. Marshall, R. Woods, Key generation from wireless channels: A review, IEEE Access 4 (2016) 614–626.
[10] R. Prabha, M.V. Ramesh, V.P. Rangan, Building optimal topologies for real-time wireless sensor networks, in: 2018 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), IEEE, 2018, pp. 1–6.
[11] M.S. Kumar, S. Kirthiga, Review of parametric radio channel prediction schemes for MIMO system, in: 2016 International Conference on Circuit, Power and Computing Technologies (ICCPCT), IEEE, 2016, pp. 1–5.
[12] V. Goutham, V. Harigovindan, Full-duplex cooperative relaying with NOMA for the performance enhancement of underwater acoustic sensor networks, Eng. Sci. Technol. Int. J. 24 (6) (2021) 1396–1407.
[13] L.H. Ozarow, A.D. Wyner, Wire-tap channel ii, AT&T Bell Lab. Tech. J. 63 (10) (1984) 2135–2157.
[14] A. Thangaraj, S. Dihidar, A.R. Calderbank, S.W. McLaughlin, J.-M. Merolla, Applications of LDPC codes to the wiretap channel, IEEE Trans. Inf. Theory 53 (8) (2007) 2933–2945.
[15] R. Gallager, Low-density parity-check codes, IRE Trans. Inf. Theory 8 (1) (1962) 21–28.
[16] J. Pfeiffer, R.F. Fischer, Multilevel coding for physical-layer security, IEEE Trans. Commun. 70 (3) (2022) 1999–2009.
[17] A. Nooraiepour, T.M. Duman, Randomized convolutional codes for the wiretap channel, IEEE Trans. Commun. 65 (8) (2017) 3442–3452.
[18] A. Nooraiepour, T.M. Duman, Randomized serially concatenated LDGM codes for the gaussian wiretap channel, IEEE Commun. Lett. 22 (4) (2018) 680–683.
[19] M. Baldi, G. Ricciutelli, N. Maturo, F. Chiaraluce, Performance assessment and design of finite length LDPC codes for the gaussian wiretap channel, in: 2015 IEEE International Conference on Communication Workshop (ICCW), IEEE, 2015, pp. 435–440.
[20] I. Tal, A. Vardy, How to construct polar codes, IEEE Trans. Inf. Theory 59 (10) (2013) 6562–6582.
[21] V.S. Kumaran, G. Ananthi, Artificial noise aided polar code with optimal jamming position for physical layer security in mondrian loss integrated rayleigh wireless relay channel, Adhoc & Sensor Wireless Networks 51.
[22] Y.-P. Wei, S. Ulukus, Polar coding for the general wiretap channel with extensions to multiuser scenarios, IEEE J. Sel. Areas Commun. 34 (2) (2015) 278–291.
[23] T.C. Gulcu, A. Barg, Achieving secrecy capacity of the wiretap channel and broadcast channel with a confidential component, IEEE Trans. Inf. Theory 63 (2) (2016) 1311–1324.
[24] Y. Zhang, Z. Yang, A. Liu, Y. Zou, Secure transmission over the wiretap channel using polar codes and artificial noise, IET Commun. 11 (3) (2017) 377–384.
[25] Y. Zhang, A. Liu, C. Gong, G. Yang, S. Yang, Polar-LDPC concatenated coding for the AWGN wiretap channel, IEEE Commun. Lett. 18 (10) (2014) 1683–1686.
[26] C. Ling, L. Luzzi, J.-C. Belfiore, D. Stehlé, Semantically secure lattice codes for the gaussian wiretap channel, IEEE Trans. Inf. Theory 60 (10) (2014) 6399–6416.
[27] R. Urbanke, B. Rimoldi, Lattice codes can achieve capacity on the AWGN channel, IEEE Trans. Inf. Theory 44 (1) (1998) 273–278.
[28] M.F. Bollauf, H.-Y. Lin, Ø. Ytrehus, On the secrecy gain of formally unimodular construction a4 lattices, arXiv preprint arXiv:2202.09236.
[29] L. Liu, Y. Yan, C. Ling, Achieving secrecy capacity of the gaussian wiretap channel with polar lattices, IEEE Trans. Inf. Theory 64 (3) (2018) 1647–1665.
[30] F. Oggier, P. Solé, J.-C. Belfiore, Lattice codes for the wiretap gaussian channel: Construction and analysis, IEEE Trans. Inf. Theory 62 (10) (2015) 5690–5708.
[31] A. Viterbi, Convolutional codes and their performance in communication systems, IEEE Trans. Commun. Technol. 19 (5) (1971) 751–772.
[32] M. Baldi, N. Maturo, G. Ricciutelli, F. Chiaraluce, Physical layer security over fading wiretap channels through classic coded transmissions with finite block length and discrete modulation, Phys. Commun. 37 (2019) 100829.
[33] Y. Liang, H.V. Poor, S. Shamai, Secure communication over fading channels, IEEE Trans. Inf. Theory 54 (6) (2008) 2470–2492.
[34] M. Bloch, J. Barros, M.R. Rodrigues, S.W. McLaughlin, Wireless information-theoretic security, IEEE Trans. Inf. Theory 54 (6) (2008) 2515–2534.
[35] P.K. Gopala, L. Lai, H. El Gamal, On the secrecy capacity of fading channels, IEEE Trans. Inf. Theory 54 (10) (2008) 4687–4698.
[36] M. Le Treust, L. Szczecinski, F. Labeau, Secrecy & rate adaptation for secure HARQ protocols, 2013 IEEE Information Theory Workshop (ITW), IEEE (2013) 1–5.
[37] J.M. Hamamreh, H. Arslan, Secure orthogonal transform division multiplexing (OTDM) waveform for 5g and beyond, IEEE Commun. Lett. 21 (5) (2017) 1191–1194.
[38] M. Yusuf, H. Arslan, Controlled inter-carrier interference for physical layer security in OFDM systems, 2016 IEEE 84th Vehicular Technology Conference (VTC-Fall), IEEE (2016) 1–5.
[39] J.M. Hamamreh, E. Basar, H. Arslan, OFDM-subcarrier index selection for enhancing security and reliability of 5g URLLC services, IEEE Access 5 (2017) 25863–25875.
[40] R.M. Yamada, A.O. Steinhardt, L. Mili, Beamforming for simultaneous energy and information transfer and physical-layer secrecy, IEEE Trans. Wireless Commun. 16 (12) (2017) 8026–8036.
[41] J.M. Hamamreh, E. Guvenkaya, T. Baykas, H. Arslan, A practical physical-layer security method for precoded OSTBC-based systems, 2016 IEEE Wireless Communications and Networking Conference, IEEE (2016) 1–6.
[42] N. Zhao, F.R. Yu, M. Li, Q. Yan, V.C. Leung, Physical layer security issues in interference-alignment-based wireless networks, IEEE Commun. Mag. 54 (8) (2016) 162–168.
[43] N. Zhao, Y. Cao, F.R. Yu, Y. Chen, M. Jin, V.C. Leung, Artificial noise assisted secure interference networks with wireless power transfer, IEEE Trans. Veh. Technol. 67 (2) (2017) 1087–1098.
[44] N. Zhao, F.R. Yu, M. Jin, Q. Yan, V.C. Leung, Interference alignment and its applications: A survey, research issues, and challenges, IEEE Commun. Surveys Tutor. 18 (3) (2016) 1779–1803.
[45] Y. Liu, L. Wang, T.T. Duy, M. Elkashlan, T.Q. Duong, Relay selection for security enhancement in cognitive relay networks, IEEE Wireless Commun. Lett. 4 (1) (2014) 46–49.
[46] M. Wijewardena, T. Samarasinghe, K.T. Hemachandra, S. Atapattu, J.S. Evans, Physical layer security for intelligent reflecting surface assisted two–way communications, IEEE Commun. Lett. 25 (7) (2021) 2156–2160.
[47] Z. Zhang, C. Zhang, C. Jiang, F. Jia, J. Ge, F. Gong, Improving physical layer security for reconfigurable intelligent surface aided NOMA 6g networks, IEEE Trans. Veh. Technol. 70 (5) (2021) 4451–4463.
[48] S. Jia, J. Zhang, H. Zhao, R. Zhang, Relay selection for improved security in cognitive relay networks with jamming, IEEE Wireless Commun. Lett. 6 (5) (2017) 662–665.
[49] H. Hui, A.L. Swindlehurst, G. Li, J. Liang, Secure relay and jammer selection for physical layer security, IEEE Signal Process. Lett. 22 (8) (2015) 1147–1151.
[50] R. Negi, S. Goel, Secret communication using artificial noise, in: IEEE vehicular technology conference, vol. 62, Citeseer, 2005, p. 1906.
[51] S. Goel, R. Negi, Guaranteeing secrecy using artificial noise, IEEE Trans. Wireless Commun. 7 (6) (2008) 2180–2189.
[52] W. Liu, M. Li, G. Ti, X. Tian, Q. Liu, Transmit filter and artificial noise aided physical layer security for OFDM systems, in: 2016 8th International Conference on Wireless Communications & Signal Processing (WCSP), IEEE, 2016, pp. 1–5.
[53] M. Hussain, Q. Du, L. Sun, P. Ren, Security protection over wireless fading channels by exploiting frequency selectivity, in: 2016 8th International Conference on Wireless Communications & Signal Processing (WCSP), IEEE, 2016, pp. 1–5.
[54] B. He, Y. She, V.K. Lau, Artificial noise injection for securing single-antenna systems, IEEE Trans. Veh. Technol. 66 (10) (2017) 9577–9581.
[55] T. Akitaya, S. Asano, T. Saba, Time-domain artificial noise generation technique using time-domain and frequency-domain processing for physical layer security in MIMO-OFDM systems, 2014 IEEE international conference on communications workshops (ICC), IEEE (2014) 807–812.
[56] E. Güvenkaya, H. Arslan, Secure communication in frequency selective channels with fade-avoiding subchannel usage, in: 2014 IEEE International Conference on Communications Workshops (ICC), IEEE, 2014, pp. 813–818.
[57] X. Li, J. Hwu, E.P. Ratazzi, et al., Using antenna array redundancy and channel diversity for secure wireless transmissions, J. Commun. 2 (3) (2007) 24–32.
[58] S. Goel, R. Negi, Secret communication in presence of colluding eavesdroppers, MILCOM 2005–2005 IEEE Military Communications Conference, IEEE (2005) 1501–1506.
[59] H.-M. Wang, T. Zheng, X.-G. Xia, Secure MISO wiretap channels with multiantenna passive eavesdropper: Artificial noise vs. artificial fast fading, IEEE Trans. Wireless Commun. 14 (1) (2014) 94–106.
[60] M. Soltani, H. Arslan, Randomized beamforming with generalized selection transmission for security enhancement in MISO wiretap channels, IEEE Access 6 (2018) 5589–5595.
[61] Y. Liu, J. Li, A.P. Petropulu, Destination assisted cooperative jamming for wireless physical-layer security, IEEE Trans. Inf. Forensics Secur. 8 (4) (2013) 682–694.
[62] Q. Xu, P. Ren, H. Song, Q. Du, Security-aware waveforms for enhancing wireless communications privacy in cyber-physical systems via multipath receptions, IEEE Internet Things J. 4 (6) (2017) 1924–1933.
[63] L. Lai, J. Hu, Y. Chen, H. Zheng, N. Yang, Directional modulation-enabled secure transmission with intelligent reflecting surface, in: 2020 IEEE 3rd

International Conference on Information Communication and Signal Processing (ICICSP), IEEE, 2008, pp. 450–453.

[64] N. Rupasinghe, Y. Yapıcı, I. Güvenç, H. Dai, A. Bhuyan, Enhancing physical layer security for NOMA transmission in mmwave drone networks, in: 2018 52nd Asilomar Conference on Signals, Systems, and Computers, IEEE, 2018, pp. 729–733.

[65] Y. Zhu, B. Mao, N. Kato, Intelligent reflecting surface in 6G vehicular communications: A survey, IEEE Open J. Veh. Technol.

[66] W.U. Khan, E. Lagunas, Z. Ali, M.A. Javed, M. Ahmed, S. Chatzinotas, B. Ottersten, P. Popovski, Opportunities for physical layer security in UAV communication enhanced with intelligent reflective surfaces, arXiv preprint arXiv:2203.16907.

[67] D.-T. Do, A.-T. Le, N.-D.X. Ha, N.-N. Dao, Physical layer security for internet of things via reconfigurable intelligent surface, Future Gener. Comput. Syst. 126 (2022) 330–339.

[68] K. Feng, X. Li, Y. Han, S. Jin, Y. Chen, Physical layer security enhancement exploiting intelligent reflecting surface, IEEE Commun. Lett. 25 (3) (2020) 734–738.

[69] Z. Tang, T. Hou, Y. Liu, J. Zhang, L. Hanzo, Physical layer security of intelligent reflective surface aided NOMA networks, IEEE Trans. Veh. Technol.

[70] J. Youn, W. Son, B.C. Jung, Physical-layer security improvement with reconfigurable intelligent surfaces for 6G wireless communication systems, Sensors 21 (4) (2021) 1439.

[71] J. Zhang, H. Du, Q. Sun, B. Ai, D.W.K. Ng, Physical layer security enhancement with reconfigurable intelligent surface-aided networks, IEEE Trans. Inf. Forensics Secur. 16 (2021) 3480–3495.

[72] Z. Tang, T. Hou, Y. Liu, J. Zhang, C. Zhong, A novel design of ris for enhancing the physical layer security for RIS-aided NOMA networks, IEEE Wireless Commun. Lett. 10 (11) (2021) 2398–2401.

[73] L. Zhai, Y. Zou, J. Zhu, B. Li, Improving physical layer security in IRS-aided WPCN multicast systems via stackelberg game, IEEE Trans. Commun. 70 (3) (2022) 1957–1970.

[74] S. Soderi, A. Brighente, F. Turrin, M. Conti, VLC physical layer security through RIS-aided jamming receiver for 6G wireless networks, arXiv preprint arXiv:2205.09026.

[75] T. Do, A.-T. Le, A. Vahid, D. Sicker, A. Jamalipour, A deep neural network for physical layer security analysis in NOMA reconfigurable intelligent surfaces-aided IoT systems.

[76] K. Sheth, K. Patel, H. Shah, S. Tanwar, R. Gupta, N. Kumar, A taxonomy of AI techniques for 6G communication networks, Comput. Commun. 161 (2020) 279–303.

[77] M.K. Tefera, Z. Jin, S. Zhang, A review of fundamental optimization approaches and the role of AI enabling technologies in physical layer security, Sensors 22 (9) (2022) 3589.

[78] L. Zhao, X. Zhang, J. Chen, L. Zhou, Physical layer security in the age of artificial intelligence and edge computing, IEEE Wirel. Commun. 27 (5) (2020) 174–180.

[79] L. Li, Y. Hu, H. Zhang, W. Liang, A. Gao, Deep learning based physical layer security of D2D underlay cellular network, China Commun. 17 (2) (2020) 93–106.

[80] X. Qiu, Z. Du, X. Sun, Artificial intelligence-based security authentication: applications in wireless multimedia networks, IEEE Access 7 (2019) 172004–172011.

[81] H.T. Thien, P.-V. Tuan, I. Koo, A secure-transmission maximization scheme for SWIPT systems assisted by an intelligent reflecting surface and deep learning, IEEE Access 10 (2022) 31851–31867.

[82] R. Achary, Internet of things (iot) security threats on physical layer security, in: Data Science and Security, Springer, 2021, pp. 39–48.

[83] A.U. Makarfi, K.M. Rabie, O. Kaiwartya, K. Adhikari, G. Nauryzbayev, X. Li, R. Kharel, Toward physical-layer security for internet of vehicles: Interference-aware modeling, IEEE Internet Things J. 8 (1) (2020) 443–457.

[84] R. Khan, S.U. Khan, R. Zaheer, S. Khan, Future internet: the internet of things architecture, possible applications and key challenges 10th international conference on frontiers of information technology, 2012 10th international conference on frontiers of information technology, IEEE (2012) 257–260.

[85] S. Khanam, I.B. Ahmedy, M.Y.I. Idris, M.H. Jaward, A.Q.B.M. Sabri, A survey of security challenges, attacks taxonomy and advanced countermeasures in the internet of things, IEEE Access 8 (2020) 219709–219743.

[86] L. Sun, Q. Du, A review of physical layer security techniques for internet of things: Challenges and solutions, Entropy 20 (10) (2018) 730.

[87] N. Srinidhi, S.D. Kumar, K. Venugopal, Network optimizations in the internet of things: A review, Eng. Sci. Technol. Int. J. 22 (1) (2019) 1–21.

[88] G. Forecast et al., Cisco visual networking index: global mobile data traffic forecast update, 2017–2022, Update 2017 (2019) 2022.

[89] C. Li, C.-P. Li, K. Hosseini, S.B. Lee, J. Jiang, W. Chen, G. Horn, T. Ji, J.E. Smee, J. Li, 5G-based systems design for tactile internet, Proc. IEEE 107 (2) (2018) 307–324.

[90] R. Chen, C. Li, S. Yan, R. Malaney, J. Yuan, Physical layer security for ultra-reliable and low-latency communications, IEEE Wirel. Commun. 26 (5) (2019) 6–11.

[91] C. Wang, Z. Li, T.-X. Zheng, H. Chen, X.-G. Xia, Robust hybrid precoding design for securing millimeter-wave iot networks under secrecy outage constraint, IEEE Internet Things J. 8 (16) (2021) 13024–13038.

[92] Z. Huang, Y. Peng, J. Li, F. Tong, K. Zhu, L. Peng, Secrecy enhancing of ssk systems for iot applications in smart cities, IEEE Internet Things J. 8 (8) (2021) 6385–6392.

[93] P. Som, A. Chockalingam, Spatial modulation and space shift keying in single carrier communication, 2012 IEEE 23rd International Symposium on Personal, Indoor and Mobile Radio Communications-(PIMRC), IEEE (2012) 1962–1967.

[94] A. Jaiswal, S. Kumar, O. Kaiwartya, N. Kumar, H. Song, J. Lloret, Secrecy rate maximization in virtual-MIMO enabled SWIPT for 5G centric iot applications, IEEE Syst. J. 15 (2) (2020) 2810–2821.

[95] B. Zhang, W. Liu, Q. Li, Y. Li, X. Zhao, C. Zhang, C. Wang, Directional modulation design under a given symbol-independent magnitude constraint for secure iot networks, IEEE Internet Things J. 8 (20) (2020) 15140–15147.

[96] X. Li, Y. Zheng, W.U. Khan, M. Zeng, D. Li, G. Ragesh, L. Li, Physical layer security of cognitive ambient backscatter communications for green internet-of-things, IEEE Trans. Green Commun. Networking 5 (3) (2021) 1066–1076.

[97] H. Wang, L. Xu, W. Lin, P. Xiao, R. Wen, Physical layer security performance of wireless mobile sensor networks in smart city, IEEE Access 7 (2019) 15436–15443.

[98] S.N. Islam, Z. Baig, S. Zeadally, Physical layer security for the smart grid: vulnerabilities, threats, and countermeasures, IEEE Trans. Industr. Inf. 15 (12) (2019) 6522–6530.

[99] M.S. Kumar, R. Ramanathan, M. Jayakumar, D.K. Yadav, Physical layer secret key generation using discrete wavelet packet transform, Ad Hoc Netw. 118 (2021) 102523.

[100] M. Kumar, R. Ramanathan, M. Jayakumar, et al., An investigation of secret key generation for physical layer security using wavelet packets, Wireless Pers. Commun. 120 (1) (2021) 701–725.

[101] K. Demestichas, N. Peppes, T. Alexakis, Survey on security threats in agricultural iot and smart farming, Sensors 20 (22) (2020) 6458.

[102] M. Gupta, M. Abdelsalam, S. Khorsandroo, S. Mittal, Security and privacy in smart farming: Challenges and opportunities, IEEE Access 8 (2020) 34564–34584.

[103] A.R. de Araujo Zanella, E. da Silva, L.C.P. Albini, Security challenges to smart agriculture: Current state, key issues, and future directions, Array 8 (2020) 100048.

[104] B.M. ElHalawany, A.A.A. El-Banna, K. Wu, Physical-layer security and privacy for vehicle-to-everything, IEEE Commun. Mag. 57 (10) (2019) 84–90.

[105] X. Wang, Moving relays in downlink multiuser networks-a physical-layer security perspective, 2018 IEEE 87th Vehicular Technology Conference (VTC Spring), IEEE (2018) 1–5.

[106] A.U. Makarfi, K.M. Rabie, O. Kaiwartya, X. Li, R. Kharel, Physical layer security in vehicular networks with reconfigurable intelligent surfaces, 2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring), IEEE (2020) 1–6.

[107] B.E. ElDiwany, A.A. Abdellatif, A. Mohamed, A. Al-Ali, M. Guizani, X. Du, On physical layer security in energy-efficient wireless health monitoring applications, in: ICC 2019-2019 IEEE International Conference on Communications (ICC), IEEE, 2019, pp. 1–7.

[108] I. Lee, The internet of things (iot): capabilities and applications for smart supply chain, in: Securing the Internet of Things: Concepts, Methodologies, Tools, and Applications, IGI Global, 2020, pp. 1557–1574.

[109] G. Khadka, B. Ray, N.C. Karmakar, J. Choi, Physical layer detection and security of printed chipless RFID tag for internet of things applications, IEEE Internet of Things Journal.

[110] L. Hu, H. Wen, B. Wu, F. Pan, R.-F. Liao, H. Song, J. Tang, X. Wang, Cooperative jamming for physical layer security enhancement in internet of things, IEEE Internet Things J. 5 (1) (2017) 219–228.

[111] G. Zhang, J. Xu, Q. Wu, M. Cui, X. Li, F. Lin, Wireless powered cooperative jamming for secure OFDM system, IEEE Trans. Veh. Technol. 67 (2) (2017) 1331–1346.

[112] M. Liu, Y. Liu, Power allocation for secure SWIPT systems with wireless-powered cooperative jamming, IEEE Commun. Lett. 21 (6) (2017) 1353–1356.

[113] B. Kailkhura, T. Wimalajeewa, P.K. Varshney, Collaborative compressive detection with physical layer secrecy constraints, IEEE Trans. Signal Process. 65 (4) (2016) 1013–1025.

[114] B. Li, W. Wu, Y. Li, W. Zhao, Intelligent reflecting surface and artificial noise assisted secure transmission of MEC system, IEEE Internet Things J.

[115] J.M. Hamamreh, M. Yusuf, T. Baykas, H. Arslan, M.A.C. Cross, PHY layer security design using ARQ with MRC and adaptive modulation, 2016 IEEE Wireless Communications and Networking Conference, IEEE (2016) 1–7.

[116] D. Kombate et al., The internet of vehicles based on 5G communications, in: 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), IEEE, 2016, pp. 445–448.

[117] R. Greenstadt, J. Beal, Cognitive security for personal devices, in: Proceedings of the 1st ACM workshop on Workshop on AISec, 2008, pp. 27–30.

[118] M.H. Yılmaz, E. Güvenkaya, H.M. Furqan, S. Köse, H. Arslan, Cognitive security of wireless communication systems in the physical layer, Wireless Commun. Mobile Comput. (2017).