Artificial Intelligence Based Physical Layer Security with Energy Harvesting in Single Hop Relaying Environment: A Survey

Pradeep Kumar, M.Tech Scholar, Department of Electronics and Communication Engineering, Kanpur Institute of Technology, Kanpur, India.

Shashank Srivastava, Assistant Professor, Department of Electronics and Communication Engineering, Kanpur Institute of Technology, Kanpur, India.

Abstract: In order to protect the secrecy of communications and provide authentication, the Physical Layer Security Protocol, also known as PHY-security, makes use of the inherent unpredictability of transmission channels. It is anticipated that technologies like as wiretapping coding and signal processing would play significant roles in this new security mechanism. PHY-security has drawn a lot of attention due to the fact that our daily lives rely largely on wireless communications for the transmission of private and sensitive information. This is one of the reasons why PHY-security has garnered so much interest. PHY-security technologies perform security functions without addressing how those security protocols are executed, in contrast to conventional cryptography, which strives to guarantee that all involved entities load proper and authenticated cryptographic information. To put it another way, it does not necessitate the implementation of any additional security techniques or algorithms on levels that are higher than the physical layer. This survey presents the fundamental theories of PHY-security, which cover confidentiality and authentication, and gives an overview of the state-of-the-art works on PHY-security technologies that can enable secure communications in wireless systems. Additionally, discussions on challenges and their proposed solutions are included in this survey as well. In addition to this, the unanswered questions that we plan to investigate in the future are outlined at the conclusion of the study. In this paper, we present an extensive literature review on the research progresses in wireless networks with RF energy harvesting capability, referred to as RF energy harvesting networks (RF-EHNs).

Index Terms—Physical layer security (PLS); Wiretap channel; Energy Harvesting; Multi-antenna systems; Relay.

1. INTRODUCTION

RF harvesting, also known as radio frequency energy harvesting or scavenging technique (see [1] and references therein), is the capability of converting the radio frequency (RF) signals that are received into electricity. Recently, there has been an upsurge of research interests in this technique, which can be shortened to RF harvesting. This method offers a potentially useful answer to the problem of providing electricity to energy-limited wireless networks. Conventionally, energy-constrained wireless networks, such as wireless sensor networks, have a limited lifetime, which mainly limitations the network performance. This problem can be alleviated, however, by employing energy-efficient techniques. In contrast, radio frequency energy harvesting networks, also known as RF-EHNs, are able to derive a reliable source of power from their surrounding radio environments. Because of this, the RF energy harvesting feature enables wireless devices to derive the energy necessary for information processing and transmission from RF signals. As a direct consequence of this, RF-EHNs have rapidly found use in a variety of contexts, such as in wireless sensor networks [2], wireless body networks [3], and wireless charging systems. As new applications for RF energy harvesting and charging continue to emerge, the Wireless Power Consortium is likewise working toward the goal of defining an international standard for the RF energy harvesting technique.

Radio signals with a frequency range that can go as low as 3 kHz and as high as 300 GHz are utilized as a channel to carry energy in the form of electromagnetic radiation when RF energy harvesting is taking place. One of the methods of wireless energy transmission is the transfer and harvesting of radio frequency (RF) energy. Inductive coupling and magnetic resonance coupling are the two other methods. The concept of inductive coupling [5] is based on magnetic coupling, and it transfers electrical energy between two coils that have been adjusted to resonate at the same frequency. The electric power is carried through the magnetic field between two coils. Evanescent-wave coupling is used in magnetic resonance coupling [6] to facilitate the generation of electrical energy and its subsequent transfer between two resonators. The resonator is produced when a capacitance is added to an induction coil in the circuit. Both of the aforementioned methods are forms of near-field wireless transmission, and both are distinguished by their high power density and efficient conversion. The coupling coefficient, which is determined by the distance that separates two coils or resonators, is directly proportional to the power transmission efficiency. Because the power's intensity is reduced by an amount proportional to the cube of the distance's reciprocal [7], [8], more specifically by 60 dB for every decade of the distance, there is a restriction placed on the distance over which it can be transmitted. In addition, calibration and alignment of the coils and resonators that are used in the transmitters and receivers is necessary for both inductive coupling and resonance coupling. As a result, you cannot use them for mobile or remote recharging or replenishment because they are not suited. In contrast, the transfer of energy through RF does not have this restriction. RF energy transmission is considered to be a method of far-field energy transfer since the radioactive electromagnetic wave cannot retroact against the antenna that created it (via capacitive or inductive coupling) over a distance greater than $\lambda/(2\pi)$ [9.] Therefore, the transfer of RF energy provides an option for powering a greater number of devices that are dispersed across a broader region. Far-field radio frequency (RF) transmissions have a signal strength that is reduced proportionally to the reciprocal of the distance between the transmitter and the receiver; more specifically, this reduction is equal to 20 decibels (dB) for every decade of the distance. The key differences and similarities between these three basic methods of wireless energy transfer are outlined in Table I. We are able to show that the RF energy transmission method possesses obvious benefits in terms of the effective energy transfer distance. However, the efficiency of the RF-to-DC energy conversion is low, and this is especially true when the amount of RF power that is captured is low. Readers interested in a more in-depth explanation of methods for wirelessly transferring energy might look at [11] and [12] respectively. The topic of wireless networks utilizing the RF energy harvesting technique plays an enormous role in this article.

Since a long time ago, researchers have been focusing their attention on wireless power transfer as a separate research challenge from wireless information transmission. Free-space beaming and antennas have traditionally been used. With huge apertures were utilized in order to get around the problem of power transfer being lost during propagation. For instance, in the 1960s, the authors of [14] exhibit a miniature helicopter that is able to hover at a height of 50 feet while being driven by a DC power supply of 270W and an RF source that is operating on 2.45GHz on the ground. [14] The authors of [15] present a demonstration of a space-to-earth power transmission system that makes use of enormous broadcast antenna arrays located on a satellite as well as receive antenna arrays located at a ground station. Over a transfer distance of 36,000 kilometers, it is estimated that the power transfer efficiency will be 45% with a transmit power of 2.7GW. The last decade saw the introduction of RF energy harvesting circuits, which led to an increase in interest in low power transfer for powering mobile terminals in wireless communication systems [16], [17]. The authors of [16] suggest a network design for RF charging stations that overlay with an uplink cellular network. This would allow the stations to communicate with one another. A harvest-then-transmit protocol is presented in reference [17] as a means of facilitating the transmission of power within a wireless broadcast system. In addition, many other current beamforming techniques are used to improve the efficiency of power transfer [17–19] for mobile applications. The dual use of radio frequency (RF) signals for supplying energy as well as for transmitting information has only lately been promoted [20-21]. For the delivery of radio frequency (RF) energy, a method known as simultaneous wireless information and power transmission (SWIPT) [22] has been developed. This method operates typically in a low power zone (e.g., for sensor networks). SWIPT provides the benefit of delivering controllable and efficient on-demand wireless information and energy concurrently, which offers a low-cost option for sustainable operations of wireless systems without requiring hardware modification on the transmitter side. SWIPT also provides the advantage of delivering both information and energy wirelessly. However, recent research has shown that improving wireless information transfer and energy transfer at the same time concurrently entails tradeoffs to the design of a wireless system [20-23]. The quantity of "variations," or the entropy rate, in an RF signal is what defines the amount of information contained in the signal, but the average squared value of RF signals is what accounts for the signal's power. This can be understood as follows: As a consequence of this, it is not possible to generally optimize both the amount of information conveyed and the amount of energy transferred at the same time. Because of this, there is a growing need for the existing wireless networks to be redesigned.

The purpose of this study is to offer a complete review of the most recent research in the field of RF-EHNs. The scope of this examination encompasses the design of circuits, the protocols that are used for communication, as well as the new designs for operations in different kinds of RFEHNs. Please take note that we place a strong emphasis on the design challenges posed by communications in RF-EHNs. The electronic hardware technology required for RF energy harvesting is outside the scope of what is covered in this paper. The primary design considerations for RFEHNs are presented in Figure 1. The survey can be broken down into the following sections. Following this, the following part will provide an overview of RF-EHNs, concentrating on the system architecture, RF energy sources and harvesting techniques, as well as existing applications.

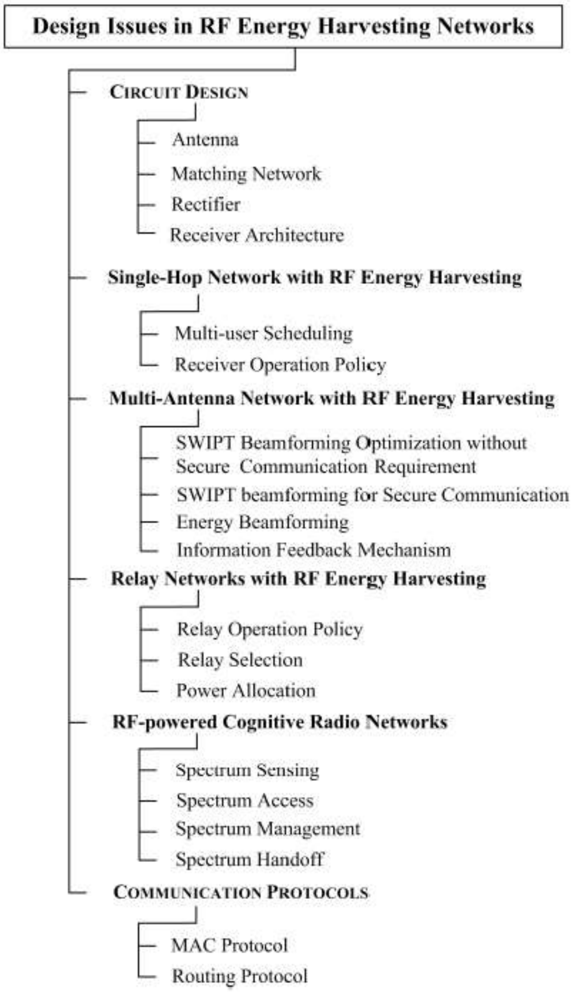
Design Issues in RF Energy Harvesting Networks
CIRCUIT DESIGN
Antenna
Matching Network
Rectifier
Receiver Architecture
Single-Hop Network with RF Energy Harvesting
Multi-user Scheduling
Receiver Operation Policy
Multi-Antenna Network with RF Energy Harvesting
SWIPT Beamforming Optimization without Secure Communication Requirement
SWIPT beamforming for Secure Communication
Energy Beamforming
Information Feedback Mechanism
Relay Networks with RF Energy Harvesting
Relay Operation Policy
Relay Selection
Power Allocation
RF-powered Cognitive Radio Networks
Spectrum Sensing
Spectrum Access
Spectrum Management
Spectrum Handoff
COMMUNICATION PROTOCOLS
MAC Protocol
Routing Protocol

Figure 1: Design Issues in RF-EHNs

Due to the fact that wireless channels engage in broadcasting, wireless communication networks are especially susceptible to assaults that involve eavesdropping and impersonation. In order to protect against these dangers, wireless communication networks must meet two fundamental security criteria. These requirements are known as authentication and secrecy. Eavesdroppers are prevented from reading sensitive messages thanks to the protection provided by confidentiality. Message recipients are able to determine the origin of a transmission thanks to authentication, which prevents any potential attacker from posing as the message's source and preventing impersonation.

In the past, traditional methods of security relied on symmetric and asymmetric cryptographic algorithms to accomplish the goals of achieving communication confidentiality and authenticating users, respectively. This paper is a survey that focuses on an alternative security mechanism called PHY-security. PHY-security is implemented on the physical layer by investigating the randomness nature of the physical layer transmission media in order to achieve both confidentiality and authentication. The paper is focused on this alternative security mechanism.

PHY-security offers a number of benefits that cannot be obtained through the use of cryptographic technologies that are implemented at higher layers. In some respects, PHYsecurity offers a higher level of protection. For instance, the physical characteristics of wireless channels can be exploited to guarantee message confidentiality with the assistance of appropriate coding and signal processing. In this scenario, it is guaranteed that only the intended receivers of confidential messages will be able to decode the messages, which protects the confidentiality of the messages. Eavesdroppers may have access to infinite computing capabilities, allowing them to launch brute force attacks or analytical attacks [21], which can be catastrophic for any cryptosystem. While there are numerous risks in cryptographic methods due to the rapid advancement of computing technologies, eavesdroppers may be able to intercept your communications. In addition, there are a number of practical approaches that can be taken to implement PHY-security. PHY-security does not need to consider how security protocols are executed, and it does not require the implementation of any additional security mechanisms on layers that are higher than the physical layer. This means that it does not consume massive communication resources or infrastructures to share cryptographic materials amongst legitimate entities [22], which is a significant time and resource savings. In addition, PHY-authentication can authenticate genuine nodes in a relatively short amount of time before demodulating and decoding signals. This allows for the avoidance of needless signal processing caused by unintentional transmissions.

PHY-security research may be traced back to Shannon's information theoretic secrecy analysis [23], which established that the level of security is dependent on the quantity of information that is already known by eavesdroppers. This is where the research first began. Eavesdroppers can attain complete secrecy if they disregard the information that is being conveyed in its entirety and instead focus on trying to guess the original information bit by bit through a process of randomization. Because of the tight relationship between this definition of security and communications in the presence of noise, the notions of entropy and equivocation that were established for communication difficulties had a direct inspiration in the early investigations on PHY-security [24–28]. When utilizing wiretap channel coding, confidential communications are able to attain a maximum message transmission rate, the rate of which is characterized as the secrecy capacity by Wyner [24]. In point of fact, all that Wyner did was demonstrate that it is possible to create secure communications even in channels with reduced broadcast quality. Since the development of non-degraded channels [9], Gaussian channels [27], small scale fading channels [28–320], multi-antenna channels [31], and relay channels [32], PHY-security ideas have gained a greater following. In addition, physical layer key generation, also known as PHYkey generation, is being increasingly recognized as a potentially useful confidential method. This method makes use of the random qualities of the physical layer in order to distribute secret keys. Raw materials that can be used to construct secret keys for two terminals include random characteristics such as channel state information (CSI) [33], received signal strength (RSS) or phase information [34], and secrecy wiretap channel codes [35]. The study has recently been expanded to authentication [36], which can defend against impersonation attacks. PHY-security can be thought of as a prototype when seen through the lens of security theory. This prototype includes secrecy and authentication in the physical layer.

2. OVERVIEW OF RF ENERGY HARVESTING NETWORKS

In this part, we will begin by providing a general overview of the architecture of an RF-EHN and then proceed to discuss the process of RF energy harvesting. The applications of RF-EHNs that are currently in use are then discussed.

The information gateways, the RF energy sources, and the network nodes or devices are the three primary elements that make up the typical centralized architecture of an RF-EHN, which is depicted in Figure 2 and includes all of these elements. Base stations, wireless routers, and relays are the common names for the various types of information gateways. Either dedicated radio frequency energy transmitters or ambient radio frequency sources can function as the RF energy sources (e.g., TV towers). The pieces of user equipment that are able to communicate with the information gateways are known as network nodes. Typically, the information gateways and RF energy sources have constant and fixed power supply, while the network nodes harvest energy from RF sources to maintain their operations. It's possible that the information gateway and the RF energy source are the same thing in some circumstances. As can be seen in Figure 2, the arrow lines with solid ends reflect information flows, whereas the arrow lines with dashed ends represent energy flows.

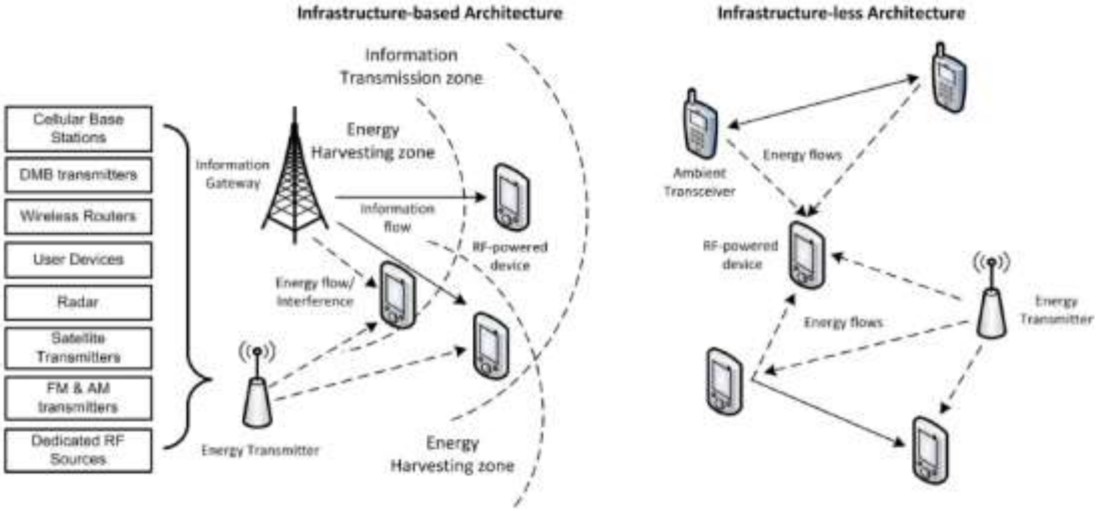

Figure 2: General architecture of an RF energy harvesting network

The energy harvesting zone and the information transmission zone are both shown by dashed circles in Figure 2. The information gateway has both of these zones. The RF energy coming from the information gateway can be collected by the devices that are located in the energy harvesting zone. The information that is being transferred from the gateway can be successfully decoded by the devices that are located in the information transmission zone. In most cases, the power required to run the energy harvesting component is far greater than the power required to run the information decoding component. As a result, the zone for the transmission of information is far larger than the zone for the collection of energy [37]. It is important to take note that the decentralized RFEHN also possesses an architecture that is comparable to the one displayed in figure 2, with the exception that the network nodes communicate with one another directly.

3. PHYSICAL LAYER SECURITY FUNDAMENTALS AND TECHNOLOGIES

The concept of PHY-confidentiality was initially presented in a model of a wiretap channel, which makes use of non-structured random codes. The fundamental goal is to increase the amount of data that can be transmitted while simultaneously placing restrictions on the amount of information that may be obtained by an eavesdropper. Even though this channel is susceptible to unpredictable ambient disturbances, the wiretap coding must still offer a reliable link between a genuine transmitter and a legitimate receiver. This link must allow information to be transferred with an arbitrarily minimal number of errors. Shannon demonstrated that reliable communication can be achieved through the use of appropriate channel coding [38]. The last thing that has to be done is to obtain an ideal secrecy capacity by utilizing efficient channel coding or signal processing so that both reliability and security are ensured. In order to achieve this goal, one common strategy involves the creation of secure non-structured random codes or structured codes, followed by the application of signal processing technologies, such as multi-antenna and relay systems, in order to establish an environment in which these codes can function in an efficient manner. Methods of PHYkey generation were offered as potential alternatives to existing mechanisms for maintaining confidentiality. The primary objective of generating PHY keys is to raise the overall level of entropy and randomness in shared channels between two terminals. The most recent techniques primarily incorporate key generation techniques that are based on CSI, RSS, phase, or wiretap codes. To determine the identities of terminals, PHY-authentication, on the other hand, makes use of pilot signals in conjunction with the characteristics of the channel. PHY-job authentication's is to protect against attacks that use pilot spoofing, therefore that's what it does. Innovative authentication methods, such as those based on CSIs, wiretap codes, radio frequency (RF) recognition, and other technologies, have been developed.

A. **Attack Models:** First, let's talk about the several types of attacks that can be carried out by an adversary, such as eavesdropping, jamming to help in eavesdropping, impersonation, and communications fabrication.

- **Eavesdropping:** Attackers who engage in eavesdropping can be divided into two categories: those who actively listen in and those who remain silent. The primary distinction between the two is that active eavesdroppers acting as communication parties are more likely to accidentally convey certain messages to transmitters. These transmitters' CSIs can be determined by CSI estimate. Silent eavesdroppers listen in on conversations without making a sound, preventing the transmission of their coded signal indicators (CSIs) to other parties.
- **Eavesdropping with assistance of jamming**: Jamming-assisted attackers look for ways to improve their ability to listen in on conversations. This attack, which seeks to broadcast jamming signals in order to minimize secrecy capacities, was researched in [39]. Recent articles [40] took a fresh look at the problem, framing it in such a way that the proactive eavesdroppers may be considered to be legitimate monitors of the situation. The proactive eavesdroppers are not interested in reducing the amount of secrecy capabilities; rather, they are interested in transmitting jamming signals in order to increase the amount of wiretap channel capacities.
- **Impersonation:** Those who steal another person's identity undermine the validity of identity-based trust. These attackers could create a large number of phoney identities or steal the identities of other legal nodes using a technique known as a Sybil attack [41]. The broadcasting nature of wireless channels makes them more susceptible to attacks of this kind, particularly on the physical layer; in the absence of medium access control and IP/IPv6 protocols, wireless channels are especially vulnerable.
- **Messages falsification:** Messages falsification degrades data-centric trust. It is possible for both internal and external attackers to change a portion of messages while they are in the process of transmission. This has the effect of undermining the faith that receivers place in the messages.

B. Wiretap Channel Models and Coding

A discrete memoryless wiretap channel model was first presented by Wyner in the year 1975 [24]. As can be seen in Figure 3, the messages are securely conveyed to Bob1 over the main channel, but the messages are kept secret from Eve in a channel that is used to wiretap conversations. Wyner gave the impression that the factors that are inherently present in physical channels, such as sounds and interferences, play important roles in the protection of communications.

Let the entropy of the message's source, S^k, be denoted by d = $H(S^k)$. The residual equivocation that Eve has regarding Sk is represented by a conditional entropy, which can be written as $H(S^k |Z^n)$. It is necessary for the rate of the coding $(2^n,R)$ to be lower than the residual entropy ratio, that is, $Rd \leq H(S^k |Z^n)/n$. This is the only way to guarantee complete confidentiality against snoopers. Wyner presented the characterization of a family of feasible pairs with the notation (R, d), and he suggested that there is a randomized codebook that maximizes R. The maximum rate of secrecy that may be maintained is referred to as the secrecy capacity Cs.

$$C_s = \max_{V \to X \to Y Z} I(V;Y) - I(V;Z) \qquad (1)$$

Where I(;) denotes mutual information, and V is an auxiliary input variable with a joint auxiliary input distribution p(s) p(v|s) p(x|v). Given a discrete memoryless channel $PY_{Z|X}$, wiretap codes achieve the secrecy capacity via maximization over the choices of the joint distribution PY Z|X, such that the Markov chain V ! X ! Y Z holds [9].

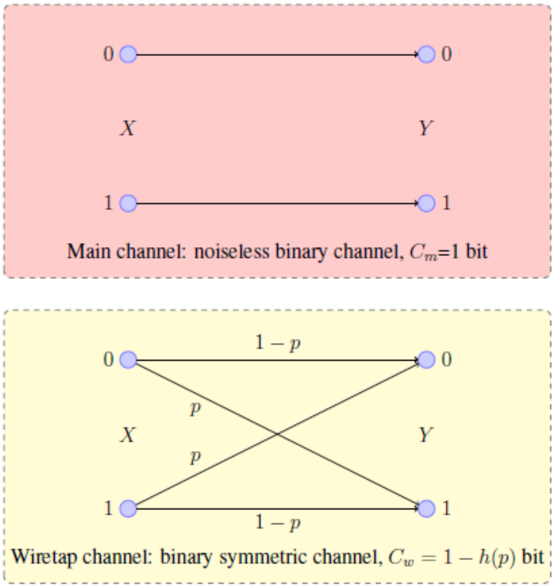
0
0
X
Y
1
1
Main channel: noiseless binary channel, C_m=1 bit
$1-p$
0
0
p
X
Y
p
1
1
$1-p$
Wiretap channel: binary symmetric channel, $C_w = 1 - h(p)$ bit

Figure 3: Example wiretap channel model

In this configuration, the primary channel is a noiseless binary channel, while the wiretap channel is a BSC with a bit error rate of *p*. Any bit that is transmitted over the main channel can be received without any kind of error, however the capacity of the wiretap channel is dependent on the value of *p*. In the scenario in which *p* = 0.5, the capacity of the wiretap is 0 bits, and the wiretap channel model is in its optimal state, with Cs = 1 bit. In the scenario when *p* = 0.1100278, the capacity for wiretapping is more than 0.5, while the capacity for maintaining confidentiality falls to a level lower than 0.5.

When the security constraint is taken into consideration, the wiretap coding rate may drop to an unacceptable level. Figure 3 illustrates the low level of secrecy that can be maintained by providing an extreme example of a wiretap channel concept. At begin, we provide a hypothetical scenario in which the primary channel is a noiseless binary channel and the wiretap channel is a binary symmetric channel (BSC) with its bit error rate (BER) set to 0.5. If this scenario plays out, it indicates that the condition of the wiretap channel is the worst possible, while the status of the main channel is the finest possible. As long as the wiretap code rate is R = 1, it has been demonstrated that the equivocation can be equal to the total binary source information entropy. This is due to the fact that h(0.5) = 1. However, when the wiretap channel becomes better as h(*p*) = 0.5, which corresponds to *p* = 0.1100278 [5,] the wiretap code rate needs to drop to less than 0.5 in order to be consistent with the binary source information entropy. This is necessary in order to maintain the integrity of the information. [8] made available a unique category of broadcast channels, in which the main channel and the wiretap channel both exhibit symmetric behaviour. It gave the difference between the conditions "a little noisy" and "more capable," and the results also showed that the wiretap code rate equals to the difference between the capacities of the two channels, which is very small. Additionally, it showed that the wiretap code rate equals to the difference between the capacities of the two channels.

C. PHY-key Generation Models

The fundamental concept behind the PHY-key generation model is to accumulate a small amount of secrecy information of channels in the process of key generation. This relies on the randomness of transmit-receive channels, such as CSI, RSS, or phase information. The PHY-key generation model was developed in order to accomplish this fundamental concept. Cumulate key generation from wiretap codes transmitted via wiretap channels is a different approach that is presented in [42] as being more practical. Despite the fact that it is difficult for wiretap coding schemes to achieve sufficient secrecy capacities in bad main channel scenarios, this is an alternative method that is presented. Figure 4 depicts a generic PHY-key generation process that is based on channel randomness and wiretap channel models. This process includes sub-processes for the extraction of randomness (both channel randomness and wiretap code randomness), quantization, information reconciliation, and privacy amplification.

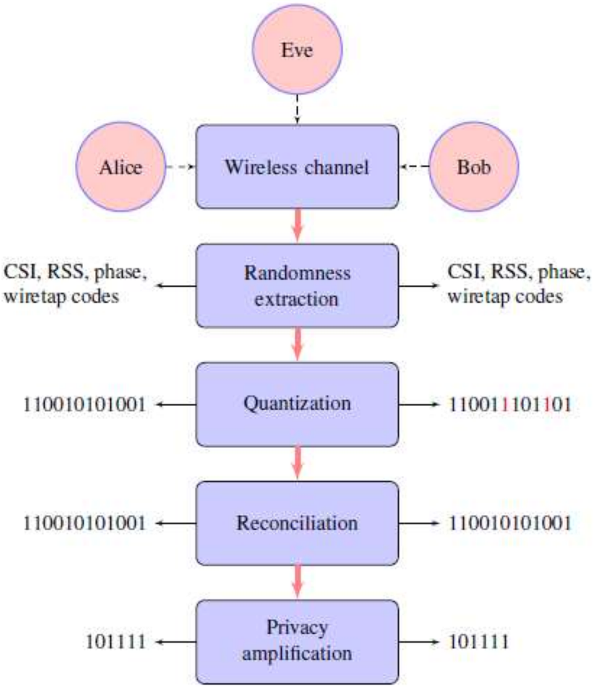

Figure 4: A general PHY-key generation model

According to this model, the two terminals are positioned so that they are at opposite ends of the same time division duplex (TDD) wireless channel that should theoretically experience the same amount of fading. Eve is separated from Bob by half a wavelength and observes channel fading that is uncorrelated with Bob's. Sub-processes devoted to randomness extraction, quantization, information reconciliation, and privacy amplification are incorporated into the generation procedure. Alice and Bob will measure CSIs, RSSs, or phase information while the randomness extraction sub-process is being carried out. When Alice and Bob are connected on the same wireless channel, the values of all of the measured parameters are theoretically the same. However, when Eve is one-half wavelength away from Bob, the values of the measured parameters can be different. Another option is for Alice and Bob to exchange opportunistic randomness through the use of wiretap codes when there is sufficient capacity for secrecy. The bits that make up the extracted randomness are quantified as a part of the process known as quantization. Alice and Bob carry out the reconciliation sub-process at the same time in order to guarantee that the keys independently created on both sides are the same. This is done to assure data integrity. The privacy amplification sub-process is a way that can either directly employ wiretap codes because Eve cannot see them or eliminate Eve's partial information about the key.

D. PHY-Authentication Models

The PHY-authentication paradigm, which is predicated on the singularity of the CSIs possessed by the medium across all transmit-receive channels [43], has its major purpose in recognizing identifying information. This is the case because the singularity of the CSIs possessed by the medium. It does channel estimation by making use of pilot signals2 and hypothesis testing in order to determine whether or not the identical transmit terminal is accountable for the most recent communication attempt as well as the one that came before it.

The assumption that Bob first stores Alice's CSI data is made by a PHY-authentication model that employs Gaussian channels. This assumption is depicted in figure 5. Bob is able to detect whether or not the terminal that is broadcasting is still

Alice once he receives additional signals since these signals allow Bob to determine whether or not the terminal is still Alice. For the purpose of channel estimation, a noisy measured version of ht is utilized, and it is this version that serves as the basis for the choice. Bob does a simple hypothesis test to assess whether the person at the transmitting terminal is Alice or a prospective invader. The test is designed to determine whether or not the individual is Alice. The findings of this examination have been reported by

$$\begin{cases} \mathcal{H}_0: & h_t = h_{ab}, \\ \mathcal{H}_1: & h_t \neq h_{ab}, \end{cases} \qquad (2)$$

If the test statistic Bob calculated indicates that ht = hab, then the null hypothesis H0, which claims that there is no intruder at the terminal, is true. He concurs with the alternative theory H1, which claims that the claimant terminal is being used by an unauthorized user, in the event that this is not the case.

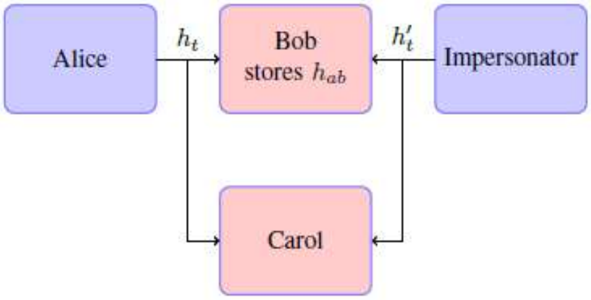

Figure 5: General PHY-authentication model

Bob, who stores the CSI between Alice and Bob, is able to verify the signal that was transmitted by Alice by doing channel estimation and hypothesis testing. Both Bob and Carol, the unknowing receiver, are capable of accurately interpreting the information, but only Bob is able to authenticate the signals. An enemy is trying to take Alice's identity by posing as her and is known as the impostor.

E. PHY-security Technologies

Several different solutions have been offered in the research that has been done on this topic in order to facilitate an easier deployment of PHY-security by increasing the transmission rate and confirming the identities of terminals. Wiretap code designs, secure multi-antenna technologies, secure relay technologies, PHY-key generation technologies, and PHY-authentication technologies are some of the possible classifications for these technologies.

Wiretap Code Designs: In accordance with the information theory on PHY-security, the most important step in the process of implementing coding is to first gain an understanding of the properties of well-known coding schemes and then to incorporate codes into increasingly complex scenarios. In addition to the non-structured wiretap coding schemes, realistic wiretap coding methods based on low-density parity-check (LDPC) coding [44] and polar coding were presented in order to accomplish the goal of maintaining anonymity.

Secure Multi-antenna Technologies: Multi-antenna systems boost wireless transmission rates by equipping both the transmitters and the receivers with numerous antennas. These antennas use space-time signal processing to send and receive data more quickly. The goal of both normal and secure multi-antenna systems is to achieve an upper bound on the secrecy capacity of multi-antenna wiretap channels. Secure multi-antenna technologies serve the same objective as normal multi-antenna systems. The differential in signal intensity between Bob and Eve needs to be increased for the multi-antenna research to be considered successful.

Secure Relay Technologies: When transmitters in multi-hop wireless networks have limited power, relay systems play a crucial role in the delivery of messages to their destinations. The ability of wireless networks to maintain their confidentiality can be improved by relays if they are used in conjunction with cooperative transmission schemes [42] such as decode and forward (DF), amplify and forward (AF), noise and forward (NF), and compress and forward (CF). When using DF methods, a relay that is collaborating with Alice will first decode messages when they are received, and then will re-encode the messages before transmitting them to Bob. When the channel from Alice to the relay has a higher level of background noise than the channel from Alice to Bob, the DF's capacity for keeping secrets is null and void. During the first interval of an AF strategy, Alice encrypts its communications before sending them to a relay. Then, during the second period, the relay will transmit a weighted version of the noisy signals that it has received, while Alice will transmit a combination of the most current and the most recent of her previous signals if there is a direct link between Alice and Bob. By doing so, the signals that are transmitted are better, which results in an increase in the ability for concealment. The relay-aided channels are transformed into two compound channels as a result of NF methods. Messages destined for Bob are transmitted by the relay in the first channel between Alice and Bob. In the second channel connecting Alice and the relay to Eve, the relay solely transmits fake signals to Eve in order to mislead her. In particular, NF strategies incorporate a deaf helper [45] in which the relay does not have to listen to Alice in order to enable a secret transmission through the generation of AN signals. This deaf helper is only used by NF strategies. It is possible to think of CF as a further generalization of NF. It is not necessary for the relay to decipher the data; all it does is delivered Bob a quantized version of the noisy observations that the relay generates. This noisy version of its observations assists Bob in deciphering Alice's messages, while the separate codewords derived from AN signals are utilized to throw off Eve's decoding efforts.

PHY-key Generation: The production of a PHY-key relies heavily on the physical layer's randomness in a substantial way. There have been four categories presented in the past two decades to discuss PHY-key generation. These four categories are CSI-based [46], RSS-based, phase-based, and wiretap code-based key generation technologies. Each of these categories is based on a different randomness property. Alice and Bob both use pilot signals in CSI-based technologies in order to get Bob-to-Alice CSI hba and Alice-to-Bob CSI hab, respectively. Because Alice and Bob suffer the same multi-path fading of a wireless link during TDD conversations, hba and hab are theoretically the same. Alice and Bob use a source coding technique to come to an agreement on a secret key that is based on hba and hab [34]. RSS-based and phase-based key generation technologies are comparable to CSI-based methods, which also use pilot signals and channel estimation methods to recover distorted RSS and phase information. RSS-based and phase-based key generation technologies use pilot signals and channel estimation methods to generate keys. On the other hand, technologies that are based on RSS and phase are more practical since they take use of channel reciprocity on RSS or phase information.

PHY-authentication Technologies: Because it functions as a digital signature to validate a transmitter's identification and should thus not be disregarded, PHY-authentication should not be overlooked. Recognizing the identities of wireless terminals on the physical layer as quickly as feasible is one of the most important aspects of PHY-authentication. CSI-based authentication, RF recognition techniques, and wiretap code-based authentication are the three technologies that are dedicated to PHY-authentication. CSI stands for cryptographic signature infrastructure. CSI-based authentication, which follows a model of embedded signalling in CSIs to fight against CSI impersonation attacks, was designed by [35]. The additional embedded signals, which provide sneaker and identifying information, can only be picked up by receivers that are aware of their presence. The RF recognition system [39] determines the identity of a device by comparing a captured emission signal from an unintentional device, such as its instantaneous amplitudes, phases, and frequencies, with the reference templates of all known devices. This comparison is performed in order to determine whether or not the device was intentionally transmitting the signal. The wiretap coding technique [46] chooses a portion of its codebook materials before sharing them between a transmitter and a receiver. In this system, the sender is verified if the receiver is able to demodulate and decode the transmission correctly.

4. CHALLENGES IN PHY-SECURITY

In wireless networks, several problems can be caused by various technologies, such as wiretap coding, secure signal processing, PHY-key generation, and PHY-authentication. These problems give rise to a number of research questions, all of which will be covered in the subsequent subsections of this article. Because Eve's CSI is unavailable in the event that Eve is a non-cooperator or a quiet eavesdropper, extra attention should be paid to the problems associated with partial CSI in each and every one of the aforementioned technologies. On the other side, fading influence makes wiretap code designs more specialized because it has the effect of reducing the capacity for concealment. However, with MIMO systems, channel fading is not considered a problem but rather a positive, as signal changes in the channels produce more degrees of freedom. This is because MIMO systems use many antennas.

- Challenges in Wiretap Code Designs
- Challenges in Secure Multi-antenna Technologies
- Challenges in Secure Relays
- Challenges in PHY-key Generation
- Challenges in PHY-authentication

5. CONCLUSION

PHY-security is a relatively young field of study in the field of security. It is anticipated that all of the devices around us will be connected thanks to advancements in communication technologies like 5G wireless networks and MTC (Machine type communication) technologies. This survey paper's main focus is on the several new PHY-security research topics that have resulted from these advances. Additionally, we have provided a thorough analysis of RF energy harvesting networks (RF-EHNs). We have first given a general review of RF-EHNs with an emphasis on their architecture, enabling technologies, and current applications. Additionally, we have emphasized intriguing research concerns associated with EH networks, such as problems with Rate-Splitting Multiple Access (RSMA) schemes and Intelligent Reconfigurable Surfaces (IRS). We think that the problems that have been revealed demonstrate that the development of security methods for EH networks is still a fascinating area of study and that it can serve as inspiration for researchers, business leaders, and start-ups who are looking for novel, non-intrusive, and computationally light ways to enforce system security in energy-restricted settings.

REFERENCES

[1] H. J. Visser and R. J. M. Vullers, “RF energy harvesting and transport for wireless sensor network applications: principles and requirements,” Proceedings of the IEEE, vol. 101, no. 6, pp. 1410-1423, June 2013.
[2] H. Nishimoto, Y. Kawahara, and T. Asami, “Prototype implementation of ambient RF energy harvesting wireless sensor networks,” in Proceedings of IEEE Sensors, Kona, HI, November 2010.
[3] X. Zhang, H. Jiang, L. Zhang, C. Zhang, Z. Wang, and X. Chen, “An energy-efficient ASIC for wireless body sensor networks in medical applications,” IEEE Transactions on Biomedical Circuits and Systems, vol. 4, no. 1, pp. 11-18, Feb. 2010.
[4] http://www.wirelesspowerconsortium.com/
[5] H. Liu, “Maximizing efficiency of wireless power transfer with resonant Inductive Coupling,” 2011. (Available on-line at http://hxhl95.github.io/media/ibee.pdf)
[6] A. Kurs, A. Karalis, R. Moffatt, J. D. Joannopoulos, P. Fisher, and M. Soljacic, “Wireless power transfer via strongly coupled magnetic resonances,” Science, vol. 317, no. 5834, pp. 83-86, June 2007.
[7] J. O. Mur-Miranda, W. Franklin, G. Fanti, Y. Feng, K. Omanakuttan, R. Ongie, A. Setjoadi, and N. Sharpe, “Wireless power transfer using weakly coupled magnetostatic resonators,” in Proc. of IEEE Energy Conversion Congress and Exposition (ECCE), Atlanta, GA, Sept. 2010.
[8] Tutorial Overview of Inductively Coupled RFID Systems, UPM Rafsec, 2003. (available online at: www.rafsec.com/rfidsystems.pdf)
[9] R. C. Johnson, H. A. Ecker, and J. S. Hollis, “Determination of farfield antenna patterns from near-field measurements” Proceedings of the IEEE, vol. 61, no. 12, pp. 1668-1694, Dec. 1973.
[10] C. Mikeka and H. Arai, “Design issues in radio frequency energy harvesting system,” Sustainable Energy Harvesting Technologies - Past, Present and Future, December 2011.
[11] N. Shinohara, “The wireless power transmission: inductive coupling, radio wave, and resonance coupling,” Wiley Interdisciplinary Reviews: Energy and Environment, vol. 1, no. 3, pp. 337-346, Sept. 2012.
[12] L. Xie, Y. Shi, Y. T. Hou, and W. Lou, “Wireless power transfer and applications to sensor networks,” IEEE Wireless Communications Magazine, vol. 20, no. 4, pp. 140-145, August 2013.
[13] A. Kurs, A. Karalis, R. Moffatt, J. D. Joannopoulos, P. Fisher, and M. Soljacic, “Wireless Power Transfer via Strongly Coupled Magnetic Resonances,” Science, vol. 317, no. 5834, pp. 8386, July 2007.
[14] W. C. Brown, “Experiments involving a microwave beam to power and position a helicopter,” IEEE Trans. on Aerospace and Electronic System, vol. AES-5, pp. 692-702, Sep. 1969.
[15] J. O. Mcspadden and J. C. Mankins, “Space solar power programs and microwave wireless power transmission technology,” IEEE Microw. Mag., vol. 3, pp. 46-57, Apr. 2002.

[16] K. Huang and V. K. N. Lau, “Enabling wireless power transfer in cellular networks: architecture, modeling and deployment,” IEEE Transactions on Wireless Communications, vol 13, no. 2, pp. 902-912, Feb. 2014.
[17] L. Liu, R. Zhang, and K. C. Chua, “Multi-antenna wireless powered communication with energy beamforming.” (available on-line at arXiv:1312.1450)
[18] G. Yang, C. K. Ho, and Y. L. Guan, “Dynamic resource allocation for multiple-antenna wireless power transfe,” IEEE Transactions on Signal Processing, vol. 62, no. 14, pp. 3565-3577, July 2014.
[19] X. Chen, X. Wang, and X. Chen, “Energy-efficient optimization for wireless information and power transfer in large-scale MIMO systems employing energy neamforming,” IEEE Wireless Communications Letters, vol. 2, no. 6, pp. 667-670, Dec. 2013.
[20] L. R. Varshney, “Transporting information and energy simultaneously,” in Proceedings of IEEE International Symposium on Information Theory, pp. 1612-1616, July 2008.
[21] X. Lu, P. Wang, D. Niyato, and Z. Han, “Resource allocation in wireless networks with RF energy harvesting and transfer,” to appear in IEEE Networks.
[22] R. Zhang and C. K. Ho, “MIMO broadcasting for simultaneous wireless information and power transfer,” IEEE Transactions on Wireless Communications, vol. 12 , no. 5, pp. 1989-2001, May 2013.
[23] P. Grover and A. Sahai, “Shannon meets Tesla: wireless information and power transfer,” in Proc. of IEEE International Symposium on Information Theory Proceedings (ISIT), pp. 2363-2367, Austin, TX, June 2010.
[24] C. A. Balanis, Antenna theory: analysis and design, John Wiley & Sons, 2012.
[25] T. S. Rappaport, Wireless Communications: Principles and Practice. Communications Engineering and Emerging Technologies. Prentice Hall, 2001.
[26] T. K. Sarkar, J. Zhong, K. Kim, A. Medouri, M. Salazar-Palma, “A survey of various propagation models for mobile communication,” IEEE Antennas and Propagation Magazine, vol. 45, no. 3, pp. 51-82, June 2003.
[27] Powercast, “www.powercastco.com”.
[28] FCC Codes of Regulation, Part 15 [Online]. Available: http://www.access.gpo.gov/nara/cfr/waisidx03/
[29] M. Erol-Kantarci and H. T. Mouftah, “Suresense: sustainable wireless rechargeable sensor networks for the smart grid,” IEEE Wireless Communications, vol. 19, no. 3, pp. 30-36, June 2012.
[30] M. Erol-Kantarci and H. T. Mouftah, “Mission-aware placement of RF-based power transmitters in wireless sensor networks,” in Proc. of IEEE Symposium on Computers and Communications (ISCC), pp. 12-17, Cappadocia, July 2012.
[31] J. Barros and M. Rodrigues, “Secrecy capacity of wireless channels,” in 2006 IEEE Inter. Sym. Inf. Theory, pp. 356–360, July 2006.
[32] P. K. Gopala, L. Lai, and H. El Gamal, “On the secrecy capacity of fading channels,” IEEE Trans. Inf. Theory, vol. 54, pp. 4687–4698, Oct 2008.
[33] Y. Liang, H. Poor, and S. Shamai, “Secure communication over fading channels,” IEEE Trans. Inf. Theory, vol. 54, pp. 2470–2492, June 2008.
[34] P. Wang, G. Yu, and Z. Zhang, “On the secrecy capacity of fading wireless channel with multiple eavesdroppers,” in 2007 IEEE Inter. Sym. Inf. Theory, pp. 1301–1305, June 2007.
[35] A. Khisti, A. Tchamkerten, and G. W. Wornell, “Secure broadcasting over fading channels,” IEEE Trans. Inf. Theory, vol. 54, pp. 2453–2469, June 2008.
[36] H. Jeon, N. Kim, J. Choi, H. Lee, and J. Ha, “Bounds on secrecy capacity over correlated ergodic fading channels at high SNR,” IEEE Trans. Inf. Theory, vol. 57, pp. 1975–1983, April 2011.
[37] M. Z. I. Sarkar, T. Ratnarajah, and M. Sellathurai, “Secrecy capacity of Nakagami-m fading wireless channels in the presence of multiple eavesdroppers,” in 2009 Conf. Signals, Systems and Computers, pp. 829–833, Nov 2009.
[38] S. C. Lin, “On ergodic secrecy capacity of fast fading MIMOME wiretap channel with statistical CSIT,” in 2013 Asia-Pacific Conf. Signal and Inf. Process. Association, pp. 1–4, Oct 2013.
[39] Z. Rezki, A. Khisti, and M. S. Alouini, “On the secrecy capacity of the wiretap channel with imperfect main channel estimation,” IEEE Trans. Commun., vol. 62, pp. 3652–3664, Oct 2014.
[40] E. Gvenkaya and H. Arslan, “Secure communication in frequency selective channels with fade-avoiding subchannel usage,” in 2014 IEEE ICC, pp. 813–818, June 2014.
[41] C. Yuen, M. Elkashlan, Y. Qian, T. Q. Duong, L. Shu, and F. Schmidt, “Energy harvesting communications: Part III [Guest Editorial],” IEEE Commun. Mag., vol. 53, no. 8, pp. 90-91, Aug. 2015.
[42] A. A. Nasir, X. Zhou, S. Durrani, and R. A. Kennedy, “Relaying Protocols for wireless energy harvesting and information processing,” IEEE Trans. Wireless Commun., vol. 12, no. 7, pp. 3622-3636, Jul. 2013.
[43] G. Chen, Y. Gong, P. Xiao and J. A. Chambers, “Physical layer network security in the full–duplex relay system,” IEEE Trans. Inf. Forensics security, vol. 10, no. 3, pp. 574-583, Mar. 2015.
[44] N. P. Ngyuyen, T. Q. Duong, H. Q. Ngo, Z. Hadzi-Velkov, L. Shu, “Secure 5G wireless communications: A joint relay selection and wireless power transfer approach,” IEEE access, vol. 4, pp. 3349-3359, 2016.
[45] J.-H. Lee, “Full-duplex relay for enhancing physical layer security in multi-hop relaying systems,” IEEE Commun. Lett., vol. 19, no. 4, pp. 525-528, Apr. 2015.
[46] N. Kumar and V. Bhatia, “Performance analysis of amplify-and-forward cooperative networks with best-relay selection over weibull fading channels,” Springer Wireless Pers. Commun (2015) 85 : 641-653.