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

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: This research explores the secrecy performance of a single hop relaying network equipped with Energy Harvesting (EH). It also demonstrates that the system equipped with EH surpasses the conventional system in terms of the secrecy rate and energy efficiency. The information signal is transmitted from the source to the destination in the presence of an eavesdropper using a relay in the system that is being proposed. Both the source and the relay make use of the time switching EH technique in order to get power from a power beacon. In this research, the secrecy rate of two cooperative schemes—decode-and-forward (DF) and amplify-and-forward (AF) for both the proposed system with EH and the traditional system is compared. These methods are decode-and-forward (DF) and amplify-and-forward (AF). At a distance of 40 metres between the eavesdropper and the relay, the system with EH gives a higher secrecy rate than the traditional system by 31.17% for DF cooperative scheme and by 24.45% for AF relay. These percentages are based on a DF cooperative scheme. In both the studied system with EH and the traditional system, the results of the study demonstrate that the secrecy rate of the AF relay is higher than that of the DF relay. This is the case regardless of which system is being analyzed. The artificial neural network method that was presented has been utilized in order to achieve better results.

Index Terms— Energy harvesting, full duplex relay, physical layer security (PLS), secrecy rate, ANN etc.

1. INTRODUCTION

In the evolution of wireless communication generations such as 1G, 2G, 3G.., International Telecommunications Union-Radio sector (ITU-R) has specified a set of requirements for 4G Communications standards [4-5]. These include namely the International Mobile Telecommunications Advanced (IMT- Advanced) specification, by setting the peak speed requirements for 4G service at 100 megabits per second (Mbit/s) for high mobility communication (such as from trains and cars) and 1 gigabit per second (Gbit/s) for low mobility communication (such as pedestrians and stationary users).

The high data rates required for Fourth Generation (5G) wireless systems in large areas do not appear feasible with the conventional cellular architecture, for two basic reasons. Firstly, the transmission rates for 4G systems are two orders of magnitude higher than those of 4G systems [6]. This demand creates serious power concerns, since it is well known that for a given transmit power level, the symbol (and thus bit) energy decreases linearly with increasing transmission rate. Second, the spectrum that is released for 5G systems will almost certainly be located well above the 2 GHz band used by the 4G systems.

The radio propagation in these bands is significantly more non line- of-sight conditions. The solution to these problems is to significantly increase the density of base stations, resulting in considerably higher deployment costs that would only be feasible, if the number of subscribers is also increased at the same rate. On the other hand, the same number of subscribers will have a much higher demand in transmission rates, by making throughput rate as the bottleneck in the future wireless systems.

A drastic increase in the number of base stations does not seem economically justifiable. It is obvious that more fundamental enhancements are necessary for the very ambitious throughput and coverage requirements of future systems. Towards this end, in addition to advanced transmission techniques and collocated antenna technologies, some major modifications in the wireless network architecture are required [7]. This is necessitated as they enable effective distribution and collection of signals to and from wireless users.

The integration of relaying with multihop capability into conventional wireless networks is the most promising architectural upgrade. While conventional cellular networks are assumed to have cells of diameter 2-5 km, a relay will only be expected to cover a region of diameter 200-500 m. The transmit power requirements for such a relay are significantly reduced compared to those of Base Station (BS). This, in turn, permits economical design of the amplifier to be used in the relay [9].

Relaying information over several point-to-point communication links is a basic building block of communication networks. Such relaying is utilized in wired and wireless networks to achieve higher network connectivity (broader coverage). Other modes are efficient utilization of resources such as power and bandwidth, better economies of scale in the cost of long-haul transmissions (through traffic aggregation), interoperability among networks, and more easily manageable, hierarchical network architectures. In wireless networks, direct transmission between widely separated radios can be very expensive in terms of transmitted power required for reliable communication [9]. High-power transmissions lead to faster battery drain (shorter network life) as well as increased interference at nearby radios. As alternatives to direct transmission, there are two basic and frequently employed examples of relayed transmission for wireless networks.

In cellular settings, for example, networks provide connectivity between low-power mobiles by providing local connections to high-power base stations that are relayed via a wire line base station network. In sensor networks, and military battlefield communication networks in general, the use of wire line infrastructure is often precluded and the radios may be substantially power constrained. However for the ad-hoc or peer-to-peer networks, transmissions can be relayed wirelessly [10-11]. Compared to adhoc networks, networks which apply relaying via fixed infrastructure do not need complicated distributed routing algorithms. While retaining the flexibility of being able to move the relays, as the traffic patterns change over time.

As these examples suggest, relayed transmission enlists two or more radios to perform multiple transmissions. The end-to-end transmissions potentially incur higher delay; but, since the individual transmissions are over shorter distances (in the wireless case), or over high-quality cabling (in the wire line case), the power requirements for reliable communication can be much lower [12].

Cooperative Relaying

Cooperative relaying is a novel technique for wireless communications promising gains in throughput and energy efficiency. The basic idea is that A device transmits a data signal to a destination [13]. A third device overhears this transmission and relays the signal to the destination as well. Finally, the destination combines the two received signals to improve decoding.

This concept gives rise to pure wireless self-organizing networks without any need of base stations. It can be employed in various applications of network embedded systems. Cars use it to communicate directly with each other, for instance, to exchange reports on accidents, traffic jams, or bad road conditions. Autonomous robots may use it to build a wireless network in areas without infrastructure, e.g., in deserts and in space.

The communication techniques, where devices cooperate to transmit signals over the air, exploit a new, distributed form of spatial diversity that mitigates the negative effects of signal fading and interference.

The task of relay selection is an important building block to realize cooperative relaying in practice. Devices located between sender and potential receiver must agree with a distributed manner as which of them will act as relay and thus promote wireless communication. The concept of cooperative relaying is a promising means to counteract the effects of small scale fading [14].

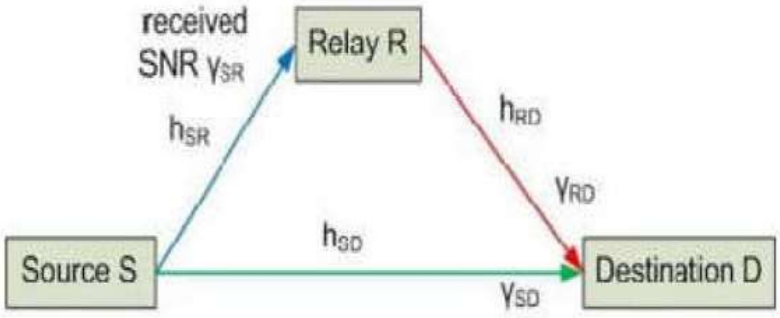

Figure 1: Cooperative relaying network

The simplest cooperative relaying network consists of three nodes, namely source, destination, and a third node supporting the direct communication between source and destination, denoted as relay. If the direct transmission of a message from source to destination is not (fully) successful, the overheard information from the source is forwarded by the relay to reach

the destination via a different path. Since the two communications take a different paths and take place one after another, this example implements the concept of space diversity and time diversity [15]. Figure 1 illustrates cooperative relaying.

Relaying Strategies

Various strategies are being employed in relaying terminals including fixed relaying method, adaptive relaying method and coded cooperative relaying method.

In fixed relaying method, the relay always forwards (a processed version) it's received message. The channel quality measurement such as the Signal to Noise Ratio measurement of the backward channel is not exploited by the relay and the later receives and processes the signal in an invariable fashion. Amplify-and-Forward relay, Decode-and-Forward relay and Estimate-and-Forward relay employ this fixed relaying strategy [16-17].

In adaptive relaying method, the relay uses a threshold rule to decide autonomously whether to forward or not. If the information of the backward channel quality is available, the relaying methods can be adaptive meaning that, the relay can adjust its behavior according to the conditions of the source-relay channel. Selection relaying and incremental relaying employ this strategy.

The coded cooperative relaying method integrates cooperation into channel coding and requires that the source and the relay transmit a part of the code word. The success of decoding can be determined by checking the cyclic redundancy code so that no feedback is required between the terminals [18]. This method can maintain the system performance and rate at the cost of added complexity at the receiver.

The fixed relaying strategies can be further distinguished by the Amplify-and-Forward, Decode-and-Forward, and Compress-and-Forward strategies.

The Amplify and Forward (AF) strategy allows the relay station to amplify the received signal from the source node and forwards it to the destination. The amplify forward relay is shown in Figure 2. Here, relays act as analog repeaters. Since a repeater amplifies whatever it receives, including noise and interferences, it is mainly useful in high signal-to-noise environments. Amplify-and-forward approach has been extended to develop space-time coding strategies for relay networks, thereby opening a new research avenue called distributed space-time coding. It is called as the scale and forward relays.

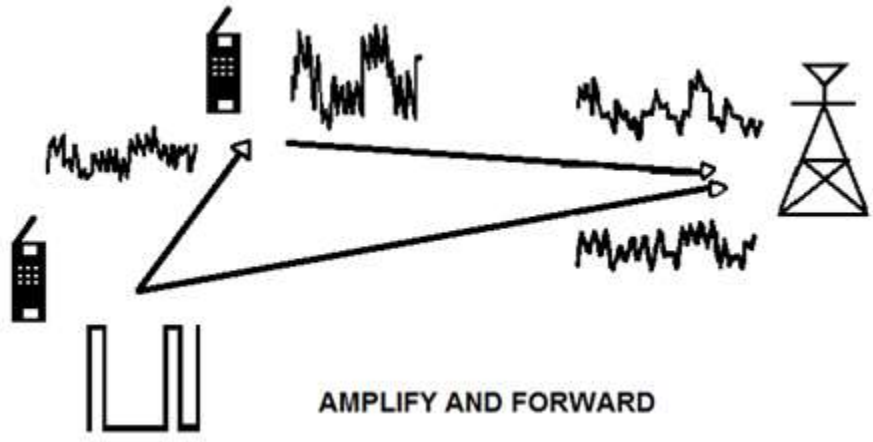

Figure 2: Amplify and forward relay network

Figure 3 shows the Decode and Forward relay. Relays following the Decode and Forward (DF) strategy overhear transmissions from the source, decode them and forward them to the destination. DF suffers from the error propagation problem which may occur, if the relay incorrectly decodes a message and forwards this incorrect information to the destination [19]. If the channel between the source and relay is corrupted with lot of noises, decode the data perfectly and forward erroneous data to the the relay cannot destination. This causes error floor in the performance and hence, the DAF protocol cannot achieve diversity. The incoming signal is just decoded and re-encoded on symbol by symbol basis. So, neither an error correction can be performed nor a checksum can be calculated. The decode and forward operation implies larger delays than simple repeaters.

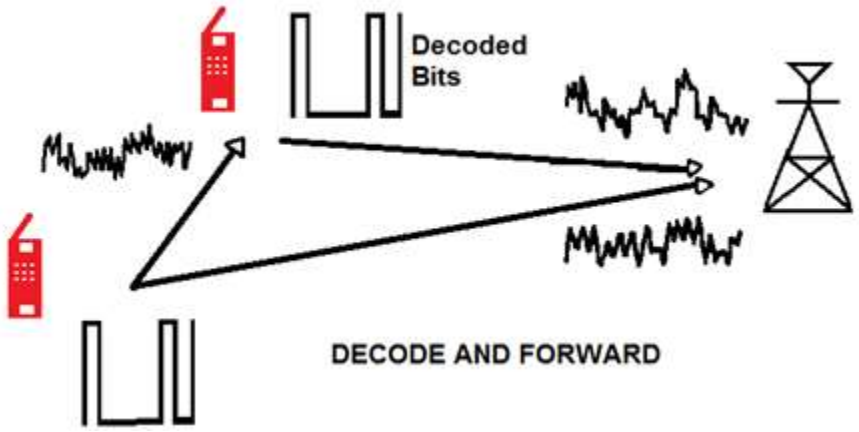

Figure 3: Decode and forward relay network

The Compress and Forward (CF) strategy allows the relay station to compress the received signal from the source node and forwards it to the destination without decoding the signal. Figure 4 shows compress and forward relay. Furthermore, the relays can operate in half-duplex mode, i.e. they do not transmit and receive simultaneously in the same band, or in full-duplex mode [20]. The latter operation requires a spatial separation between transmit and receive antennas to reduce loop-back interference from the transmit antennas to the receive antennas.

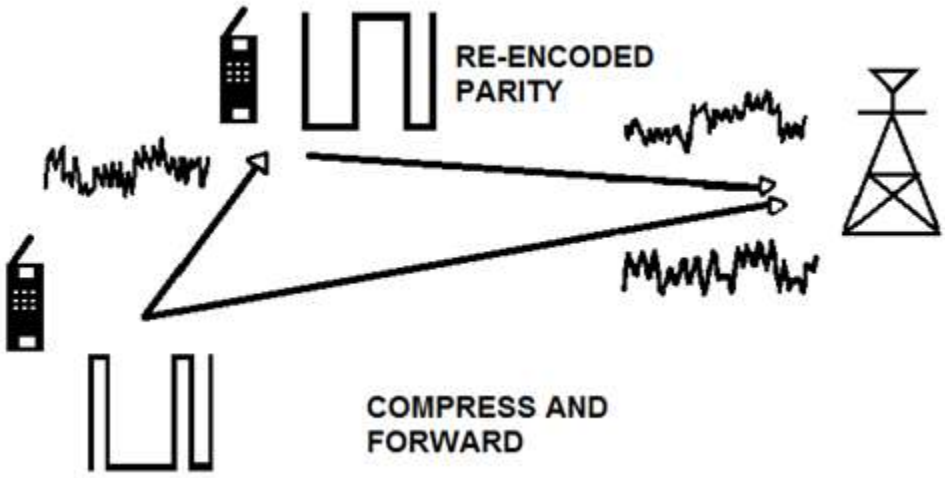

Figure 4: Compress and forward relay network

The advantages of using relays are

- Relaying technique is capable of extending communication range and coverage by providing link to shadowed users through relay nodes.
- Relays can be viewed as a virtual antenna array that provides spatial diversity to combat frequency/time fading of channels
- Increase in throughput.

Channel State Information

In wireless communication, Channel state information refers to known channel properties of a communication link. This information describes how a signal propagates from the transmitter to the receiver and represents the combined effect of, for

example, scattering, fading, and power decay with distance. The CSI makes it possible to adopt transmissions to current channel conditions, and it is crucial for achieving reliable communication with high data rates in multi antenna systems [21].

CSI needs to be estimated at the receiver and it is usually quantized and fed back to the transmitter. Therefore, the transmitter and receiver can have different CSIs. The CSI at the transmitter and the CSI at the receiver are at times referred as CSIT and CSIR, respectively.

The term "outdated" refers to the case where the CSI is correct at the time of estimation, but corresponds to a different channel realization than the channel realization at the time when it is used. As a result, outdated CSI pertains to a subset of the practical scenarios that are associated with the versatile term "imperfect" CSI.

Physical Layer Security

The idea behind physical-layer security is to utilize the physical characteristics of the communication channel to enhance communication security via suitable coding and signal processing. PLS is founded on information theoretic proofs of perfect secrecy, a concept coined by Shannon in 1949 [17]. Information Theoretic Security is a key tool for investigating the PLS. The information theoretic method is seen as a potential technique for achieving secure communication. It has the ability to significantly increase the level of security for both existing 5G and next-generation communication networks. This chapter provides an overview of information theoretic security, from the pioneering key-based Shannon work through the key-less Wyner work.

Fundamental Behind Secrecy

Any communication is built on the principle of secrecy. Specifically, this issue occurs when a transmitter (Alice) transmits confidential information to a legitimate recipient (Bob), but does so in the presence of an unauthorized user, such as an eavesdropper or a wiretapper (Eav), who intercepts the transmitted signals. In the field of information theory, secrecy research can be divided into two broad categories:

- **Secrecy With Key Based Approach**

The Shannon's Wireless Security Model: This is referred to as Shannon's wireless security model. Claude Shannon coined the term"perfect secrecy" in 1949 [17]. This perfect secrecy was obtained by assuming that legitimate users shared a key in a noiseless crypto-system Figure 6. He demonstrated that the information theoretic security can be achieved in the presence of an eavesdropper between two legitimate nodes that share a non-reusable secret key. The scheme depicted in Figure 1 is a symmetric secret key encryption scheme. The objective in this case is to reliably convey data from Alice to Bob while maintaining data secrecy from Eav. To accomplish this, it is assumed that Alice and Bob have a secret key that Eav is unaware of. A secret word (also known as a codeword) is used to encode the input message at the Alice end, and to decode the codeword back into message at Bobs' end, with this key being used in both cases. Specifically, the random variables W, C, and K are used to represent the input message, the codeword, and the keys, respectively. To maintain absolute secrecy, the message W must be statistically independent of the Eav intercepted codeword C. In other words, the mutual information I (W;C) between the message and the codeword intercepted by Eav is zero [17].

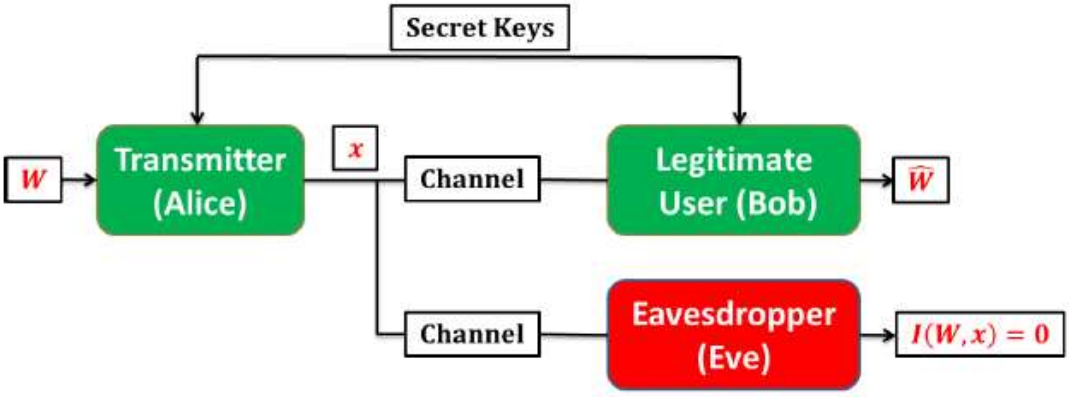

Figure 5: System model of Shannon's cipher system

- **Secrecy With Key Less Approach**

The Wyner's Wireless Security Model: b Wyner [22] came up with the idea of gaining the secrecy capacity over a degraded broadcast channel early in 1975. In this case, the channel is also seen as being noisy. It is the central concept of his work [22] to demonstrate that sensitive information can be transferred safely without the use of any encryption keys. On the basis of information theory, he established that perfect secrecy can be attained if the wiretap link quality is a degraded version of the legitimate link quality. As illustrated in Figure 7, Alice and Bob communicate using a discrete memoryless broadcast channel, which allows them to keep their message completely hidden from Eav. The entire conversation is carried out without the exchange of encryption keys.

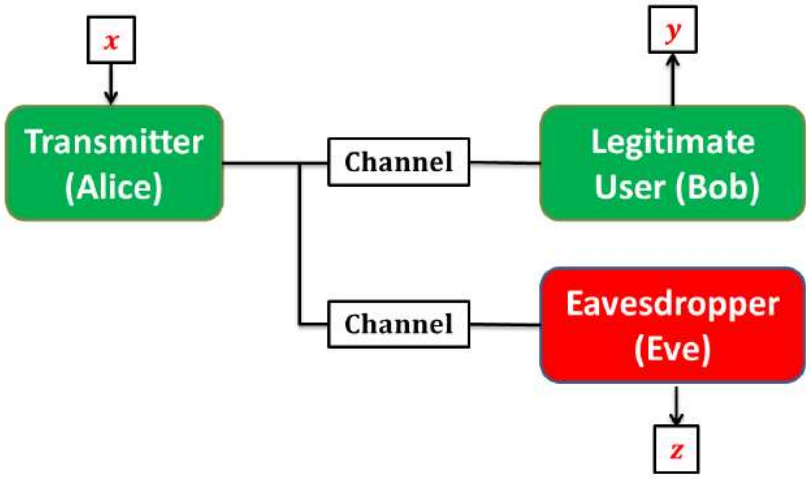

Figure 6: System model of Wyner's wiretap channel

Basic Cooperative Network

Direct transmission refers to the transmission of messages over a direct channel between the source and the destination, whereas co-operative or relay-based transmission refers to the transmission of messages with the assistance of relay nodes between the source and the destination. In Figure 6, a classic co-operative wireless network is depicted, in which a relay (R) node assists in the transfer of information from a source (S) node to a destination (D) node is demonstrated. Following the description, a three terminal network is one in which the relay simply receives the source transmitted signal, processes it according to specified protocols, and then retransmits the signal to the destination [23]. In order to send the signal from S to D, this system typically requires two phases: Phase 1 is comprised of the node S transmitting its information to the nodes R and D, while Phase 2 is comprised of the node R relaying its received signal to the destination by the use of a specific relaying protocol. The relay's processing of the incoming signal is an important part of relay-based communication. These various processing algorithms result in a variety of cooperative communications protocols. The relaying protocol can be either amplify-and-forward (AF) or decode-and forward (DF). According to the AF protocol-based relaying transmission, the relay simply amplifies the incoming signal in order to increase its power so that it can reach the destination without loss [22]. The relay node, on the other hand, in a DF protocol-based relaying transmission decodes the incoming signal before retransmitting it to the appropriate destination node. It is possible to deduce that the channel capacity of the DF protocol-based relaying network is greater than the channel capacity of the AF protocol [23] when these two protocols are compared.

In co-operative communication, the nodes share their resources to make easy communication with one another. Using relay-based communication, one can replace long-distance and low energy connections with shorter-distance and higher-energy connections. Moreover, this network provides robustness against fading communication channels [32]. According to the research [31], the relay-based co-operative network improves both the overall system capacity and the overall system diversity. The capacity of this network was initially explored by the authors in [31], who also provided upper and lower bounds for the channel capacity in the process.

Relay

Relay transmission has been widely studied [20], since it can expand the coverage and enhance the system performance. Many relay protocols have been proposed such as amplify-and-forward (AF), decode-and-forward (DF), and compress-and-forward (CF) etc. In this paper, AF and DF are considered.

Amplify-and-Forward

In AF protocol, the source first transmits the signal to the relay, then the relay amplifies the signal and forwards the signal to the destination. The secrecy rate is zero. Therefore, in two-hop untrusted relay networks, secrecy cannot be achieved for AF transmission. Cooperative jamming is an appealing scheme to achieve positive secrecy rate in two-hop untrusted relay networks [17].

Decode-and-Forward

In DF protocol, relay first decodes the signal from the source, then re-encodes it and forwards it to the destination [39]. Therefore, the untrusted DF relay cannot be employed to help forward confidential signals.

Energy Harvesting

Prolonging the lifetime of a wireless network through energy harvesting has received significant attention very recently [12]. Though, replacing or recharging batteries can avoid energy harvesting, it incurs a high cost and can be inconvenient or hazardous (e.g., in a toxic environments), or highly undesirable (e.g., for sensors embedded in building structures or inside the human body) [12]. In such scenarios, a safe and convenient option may be to harvest the energy from the environment. Apart from the conventional energy harvesting methods, such as solar, wind, vibration, thermoelectric effects or other physical phenomena [21], a new emerging solution is to avail ambient radio-frequency (RF) signals. The advantage of this solution lies in the fact that RF signals can carry energy and information at the same time. Thus, energy constrained nodes can scavenge energy and process the information simultaneously.

Energy Harvesting in Wireless Communications

Radio frequency (RF) energy harvesting (EH) has recently attracted considerable attention in the field of wireless communication. This technology becomes a solution to prolong the life-cycle of in-accessible battery-limited devices. The EH concept is based on the fact that RF signals, those in the frequency range 3 kHz to 300 GHz, can be used to carry information and energy at the same time. The amount of power that can be harvested in a wireless system is dependent on many parameters, such as the transmitted power from the RF source, the distance between the EH receiver and the RF source, path loss exponent and the EH receiver efficiency. Hence, the harvested power is Ph = Pr$P_h = P_r$ŋ where P_r is the received power and ŋ is the EH efficiency. Therefore, based on this RF-EH technique, all the devices in future wireless networks are predicted to be energy self-sufficient by harvesting energy from the RF signals and other natural sources in the surrounding environment [22].

Simultaneous Wireless Information and Power Transfer (SWIPT)

The SWIPT technique is based on the fact that RF signals can carry information and energy at the same time, hence allowing energy constrained nodes to harvest energy and process information simultaneously [25]. The concept of the SWIPT technique was first developed in [24], where a trade-off between the rates at which energy and reliable information signals can be sent over a noisy channel is considered. This work is extended in to incorporate the impact of frequency selective channels with AWGN. However, these works assume an ideal receiver which implies that decoding the information signal and harvesting energy is achieved simultaneously from the same received signals. Practically, this assumption might be un-realistic due to practical circuit design limitations. In this context, several practical receivers for information processing and energy harvesting have been proposed in the literature.

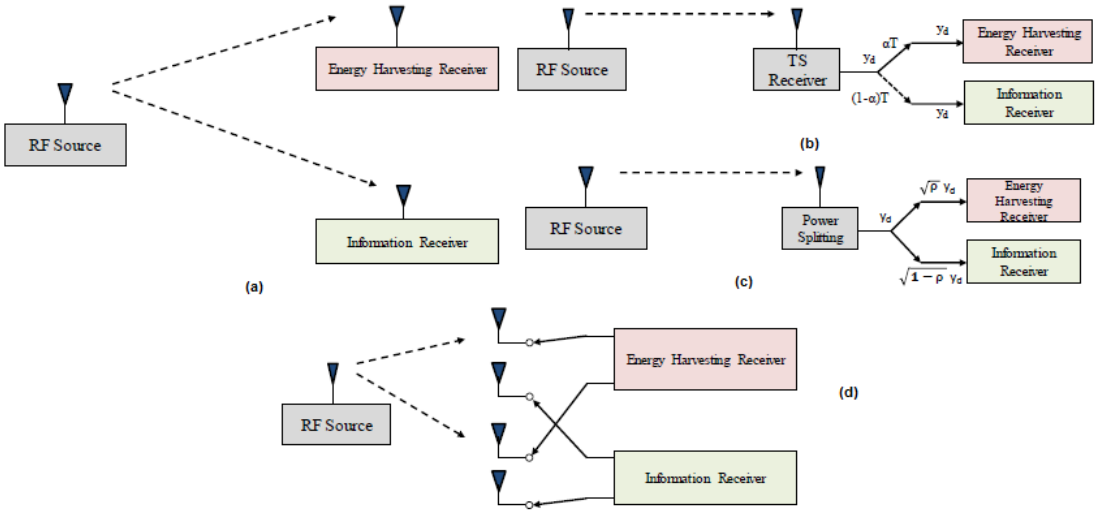

Figure 7: SWIPT receiver structures

Wireless Power Communication Networks (WPCNs)

In wireless power communication networks (WPCNs), the information transmission in the network is in the opposite direction of the wireless energy transfer, as shown in figure 9. Furthermore, in WPCNs the users cannot harvest energy and process information from the same signal simultaneously, unlike in SWIPT networks, hence a time switching strategy should be adopted in these kinds of networks.

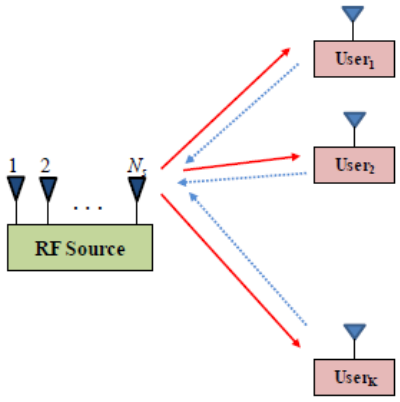

Figure 8: Example of WPC system

2. LITERATURE REVIEW

Pietro Tedeschi, Savio Sciancalepore, and Roberto Di Pietro [29] Recent improvements in hardware downsizing capabilities have accelerated the adoption of Energy Harvesting (EH)-based systems as a way to power embedded wireless devices in an economical and sustainable manner. The limited power supply and irregular energy source availability have complicated system trade-offs, increasing the attack surface and generally relaxing the accessible security services despite the undeniable management advantages. In this paper, we provide an overview of the security concerns, applications, issues, and approaches that emerge in wireless networks using EH technologies. Of addition to examining the flaws in EH networks, we also give a thorough analysis of the scientific literature, covering attack methods, cryptographic procedures, physical-layer security protocols for data secrecy, and extra physical-layer defences. We analyse the scientific contributions made to each of the identified macro-areas based on a number of common traits, highlighting the advantages and disadvantages of the approaches mentioned, the difficulties in the field, and some potential future possibilities. Finally, we give a brief overview of some recent developments in the field that have the potential to spark interest in both industry and academia and fully

realise the potential of ubiquitous EH wireless networks. These include the Rate-Splitting Multiple Access (RSMA) and Non-Orthogonal Multiple Access (NOMA) schemes.

Ali A. Nasir, Xiangyun Zhou, Salman Durrani, and Rodney A. Kennedy, [30] Utilizing the ambient radio-frequency (RF) signal while concurrently gathering energy and processing information is a newly developed method for extending the lifespan of relay nodes in wireless networks that are energy constrained. This study examines an amplify-and-forward (AF) relaying network, in which a relay node with limited energy collects energy from an RF signal and uses it to transmit data from the source to the target. Two relaying protocols, I time switching-based relaying (TSR) protocol and ii) power splitting-based relaying (PSR) protocol, are developed to enable energy harvesting and information processing at the relay. These protocols are based on the time switching and power splitting receiver architectures. Analytical equations for the outage probability and the ergodic capacity for the delay-limited and delay-tolerant transmission modes, respectively, are derived in order to calculate the throughput. The numerical analysis offers useful explanations of how different system parameters, including energy harvesting time, power splitting ratio, source transmission rate, source to relay distance, noise power, and energy harvesting efficiency, affect the effectiveness of wireless energy harvesting and information processing using AF relay nodes. Particularly, the TSR protocol surpasses the PSR protocol in terms of throughput at high transmission rates and low signal-to-noise ratios.

Xiao Lu, Ping Wang, Dusit Niyato, Dong In Kim, and Zhu Han [31] Techniques for transferring and harvesting radio frequency (RF) energy have recently emerged as alternatives for powering the next generation of wireless networks. This cutting-edge technology benefits applications with quality of service (QoS) requirements since it enables proactive energy replenishment of wireless devices. In this article, we give a thorough literature analysis on the developments in wireless networks with the potential to harvest RF energy, also known as RF energy harvesting networks (RF-EHNs). We first give a general overview of RF-EHNs, describing their system architecture, methods for harvesting RF energy, and currently used applications. Following that, we discuss the history of circuit design, the most recent circuitry implementations, and the communication protocols specifically created for RF-EHNs. In accordance with the network types, such as single-hop networks, multi-antenna networks, relay networks, and cognitive radio networks, we also examine many important design difficulties in the creation of RF-EHNs. Last but not least, we see a few open study directions.

Yiliang Liu, Hsiao-Hwa Chen, and Liangmin Wang, [32] To establish communication confidentiality and authenticity, physical layer security (PHY-security) makes use of the benefits provided by the randomness of the transmission media's channel. Technologies for signal processing and wiretap coding are anticipated to be key components of this new security system. Due to its distinctive qualities and the fact that we rely extensively on wireless communications in our daily lives for the transmission of private and sensitive information, PHY-security has received a lot of attention. PHY-security technologies carry out security functions without taking into account how those security protocols are executed, in contrast to conventional cryptography, which works to ensure all involved entities load appropriate and validated cryptographic information. In other words, no additional security algorithms or methods need to be implemented on layers above the physical layer. This survey provides an overview of current research on PHYsecurity technologies that can provide secure communications in wireless systems, as well as discussions on challenges and their potential solutions. It introduces the basic theories of PHY-security, covering confidentiality and authentication. Additionally, the outstanding issues are listed as our future study directions at the conclusion of the publication.

3. SYSTEM MODEL

The model of the system that is being considered can be seen in figure 9. This model is based on a two-hop relaying system that consists of a single-antenna source node trying to send information signals to a single-antenna destination node via antenna AF relay while there is also a single-antenna passive eavesdropper present. On the one hand, both the source and the destination each use a constant transmission power supply, designated by the letters Ps and Pdn, respectively, in order to send information and AN (Artificial Noise) signals. On the other hand, the relay is an EH node that relies only on the RF harvested energy, Eh, that it possesses in order to both amplify and forward the signal that it has received [17].

Figure 9 provides an illustration of the system model. A power beacon *B*, a source *S*, a relay *R*, a destination *D*, and an eavesdropper *E* are the components that make up this system. Let h_{BS}^*, h_{BR}^*, h_{SR}^*, h_{RD}^*, h_{SE}^*, and h_{RE}^* illustrate complex channel gains between *B* and *S*, *B* and *R*, *S* and *R*, *R* and *D*, *S* and *E*, and *R* and *E*, respectively. At each node, it is assumed that the noise is of the complex additive white Gaussian noise (AWGN) variety, with a variance of σ^2 and a mean of zero. In addition to that, the relay in this system is capable of operating in both full and half duplex mode [8].

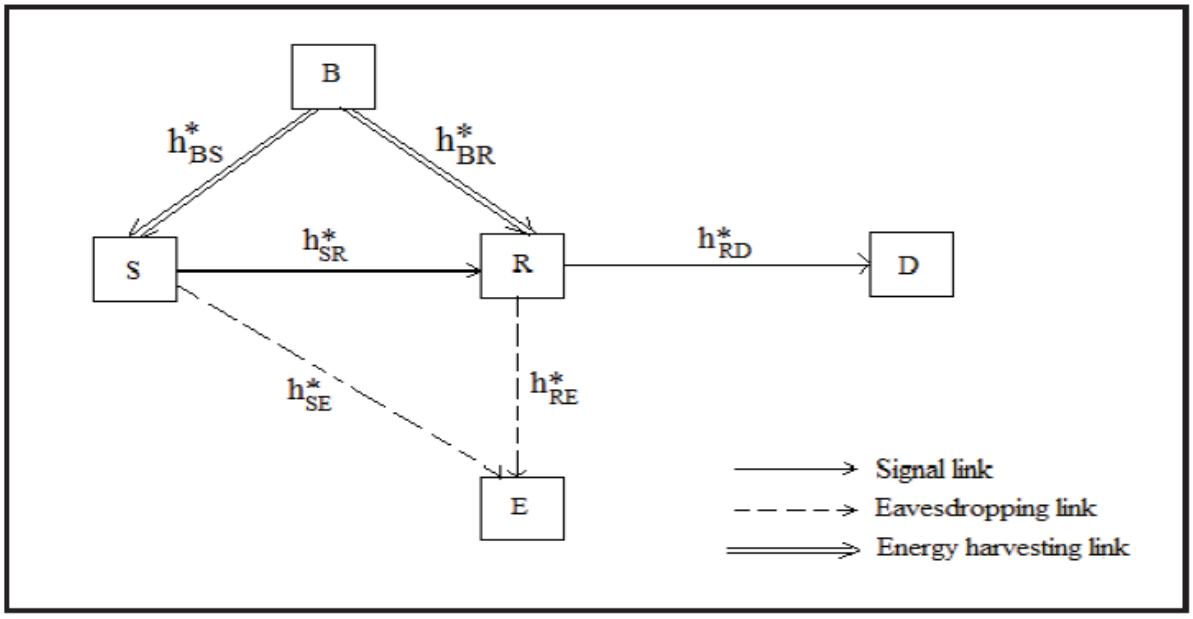

Figure 9: System Model relaying using EH

Energy Harvesting Technique

Within this particular setup, *R* and *S* are responsible for powering the signal transmission process by harvesting energy from *B*. Due to the time switching based EH protocol's high throughput, as can be seen in figure 10, it has been chosen to be utilized in this thesis. [19] and [20] are the expressions that indicate the energy that was harvested at *S* and *R*, respectively.

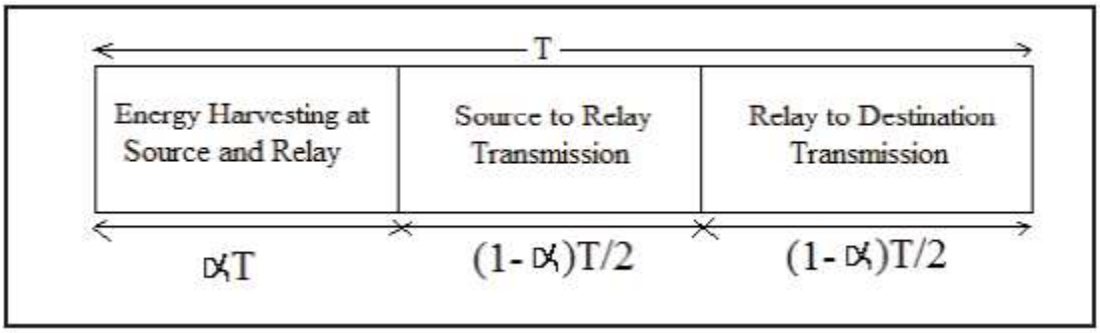

Figure 10: Time Switching Relaying (TSR) Protocol

$$E_S = \eta P_B \alpha T |h^*_{BS}|^2 \qquad (1)$$

$$E_R = \eta P_B \alpha T |h^*_{BR}|^2 \qquad (2)$$

Where, the efficiency of this technique of energy conversion is given by $0< \eta< 1$, the power sent by beacon node is given by P_B and $0 <\alpha< 1$. T represents time duration to transmit a particular block from *S* to *D*. Nodes *S* and *R* harvest energy from *B* for time period of αT. Power transmitted by *S* and *R* in this system are represented by

$$P_S = \frac{2\eta P_B |h^*_{BS}|^2 \alpha}{1-\alpha} \qquad (3)$$

$$P_S = \frac{2\eta P_B |h^*_{BR}|^2 \alpha}{1-\alpha} \qquad (4)$$

DF Scheme

It does its work in two-steps. The first step is shown in Figure 11, where the source sends the signal *x(n)* to the relay. The relay provides jamming signal *q(2n)* to the eavesdropper, at the same instant. The signals obtained at nodes *R* and *E*, in the time sloti2n are given by [17]

$$y_R(2n) = \sqrt{P_S}\, h_{SR}^* x(n) + n_R(2n),$$

$$y_E(2n) = \sqrt{P_S}\, h_{SE}^* x(n) + \sqrt{P_{RJ}}\, h_{RE}^* q(2n) + n_E(2n) \qquad (5)$$

Where, the jamming signal power of *R* is given by P_{RJ} and AWGN at *R* and *E* are represented by *nR* (*2n*) and *nE* (*2n*), respectively.

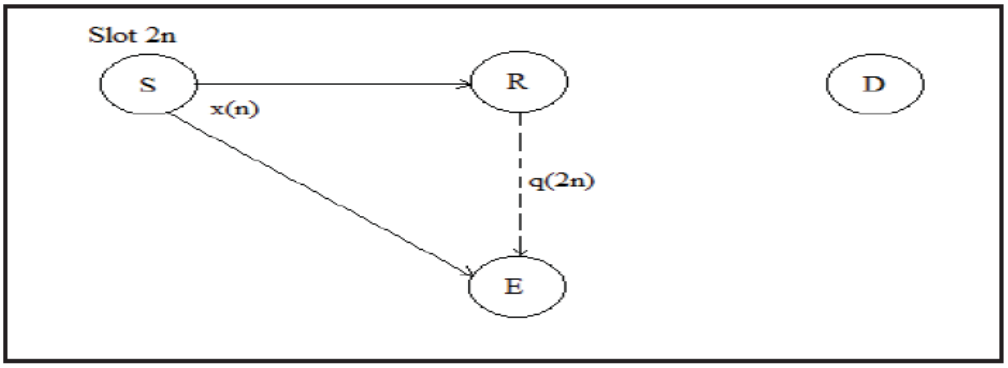

Figure 11: Illustration of signals sent in (2n)th time slot

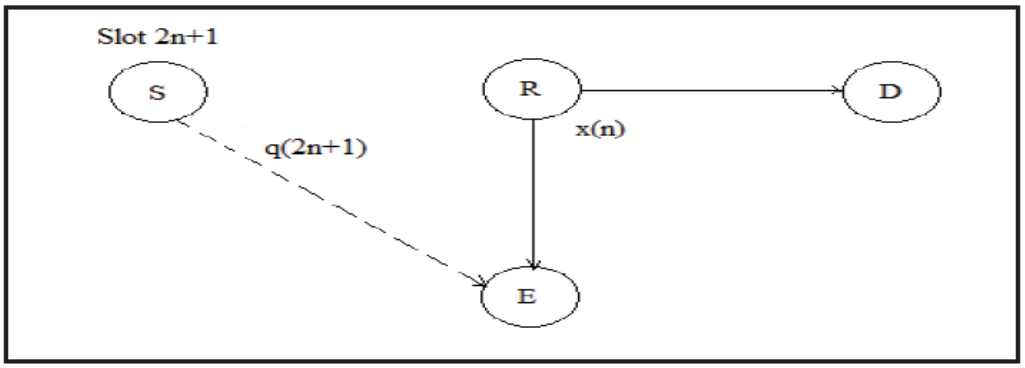

Figure 12: Illustration of signals sent in (2n+1)th time slot

The second step is shown in the figure 12, where the relay sends the previously decoded signal to the destination. Further, in this step, source sends jamming signal to the eavesdropper. The signals obtained at *E* and *D* in the time slot (2n+1) are denoted as [17].

$$y_E(2n+1) = \sqrt{P_S}\, h_{SE}^* x(n) + \sqrt{P_{SJ}}\, h_{SE}^* q(2n+1) + n_E(2n+1),$$

$$y_D(2n+1) = \sqrt{P_R}\, h_{RD}^* x(n) + n_D(2n+1) \qquad (6)$$

Where, the power of the jamming signal of *S* is represented by P_{SJ} and $n_D(2n+1)$ represents the AWGN at *D*.

AF Scheme

In a manner analogous to the DF approach, it likewise consists of two stages. The first step is exactly the same as it is in the DF approach, which can be seen in Figure 3. The equation that describes the signals that can be obtained at nodes *R* and *E*

during the first time slot 2n is as follows: (5). The second stage consists of the source amplifying the signal that it has received and then transmitting the signal that has been amplified to the location that is being communicated to. As can be seen in figure 12, the source also transmits a signal that jams the reception of the eavesdropper. The signals that were collected at *D* and *E* during the 2n+1st time slot can be represented by the symbol [18].

$$y_D(2n+1) = G\sqrt{P_S}\, h_{RD}^{*}\, y_R(2n) + n_D(2n+1),$$

$$y_E(2n+1) = G\sqrt{P_S}\, h_{RE}^{*}\, y_R(n) + \sqrt{P_{SJ}}\, h_{SE}^{*} q(2n+1) + n_E(2n+1) \qquad (7)$$

Where scalling factor $G = \frac{1}{\sqrt{P_S|h_{SR}|^2+N_0}}$ and noise variance is given by N_0.

System Secrecy Rate

The secrecy rate is the performance indicator for the physical layers of security. This rate is expressed in terms of the difference between the capacity of the direct link (which connects the source and the destination) and the capacity of the eavesdroppers' link. The secrecy rate is the pace at which the source securely sends the data to the destination in the presence of eavesdroppers. This rate is expressed in bits per second. The rate of secrecy measured in terms of the chance of information leakage that occurs when an eavesdropper is unable to decode the information collected from the source.

DF Scheme

Using equation (3.5) and (3.6), the rates at *D* and *Ei*is given by [17]

$$R_d = \frac{1}{2} log2(1 + P_R \alpha_{RD}) \qquad (8)$$

$$R_e = \frac{1}{2} log2\left(1 + \frac{P_S\, \alpha_{SE}}{1+P_{RJ}\, \alpha_{RE}} + \frac{P_R\, \alpha_{RE}}{1+P_{SJ}\, \alpha_{SE}}\right) \qquad (9)$$

Where $\alpha_{RD} = \frac{|h_{RD}|^2}{\sigma^2}$, $\alpha_{SE} = \frac{|h_{SE}|^2}{\sigma^2}$ and $\alpha_{RE} = \frac{|h_{RE}|^2}{\sigma^2}$. By using equation (8) and (9), the secrecy rate that can be achieved, is represented as

$$R_S = max\{R_d - R_e, 0\},$$

$$(R_d - R_e) = \frac{1}{2} log2\left[\frac{1+P_R\alpha_{RD}}{1+\frac{P_S\, \alpha_{SE}}{1+P_{RJ}\, \alpha_{RE}}+\frac{P_R\, \alpha_{RE}}{1+P_{SJ}\, \alpha_{SE}}}\right] \qquad (10)$$

AF Scheme

Utilizing equation (5) and (7), At *D* and *E*, the rates can be represented as [17]

$$R_d = \frac{1}{2} log2(1 + G^2 P_S \alpha_{RD}) \qquad (11)$$

$$R_e = \frac{1}{2} log2\left(1 + \frac{P_S\, \alpha_{SE}}{1+P_{RJ}\, \alpha_{RE}} + \frac{G^2\, P_S\, \alpha_{RE}}{1+P_{SJ}\, \alpha_{SE}}\right) \qquad (12)$$

The secrecy rate is given as

$$R_S = max\{R_d - R_e, 0\}$$

$$(R_d - R_e) = \frac{1}{2} log2 \left[\frac{1+G^2 P_S \alpha_{RD}}{1+\frac{P_S \alpha_{SE}}{1+P_{RJ} \alpha_{RE}} + \frac{G^2 P_S \alpha_{RE}}{1+P_{SJ} \alpha_{SE}}} \right] \quad (13)$$

4. PROPOSED METHODOLOGY

An Artificial Neural Network (ANN) could be used to alter the weights and thresholds of a connectionist model by training datasets to map input and output variables. ANNs strive to get good results by connecting a large number of neurons together. An ANN model is identified by its architecture, which includes a sophisticated algorithm for training datasets. The network architecture defines the pattern of neuronal connections, whereas the activation function defines the type of unit. There are two modes of operation for the neural network: processing and training. Algorithms define how the neural units generate results for a certain set of inputs and weights in process mode. Algorithms define how the network adjusts its weights for all coaching patterns in coaching mode [26].

KNN CLASSIFIER

The kNN classifier, for example, is based on the assumption that the categorization of unknown instances is frequently done by linking the unknown to the familiar using some distance/similarity function. The intuition is that two instances that are so far apart in the instance space described by the appropriate distance function are less likely to belong to the same category than two instances that are close together. The goal of the k Nearest Neighbors (kNN) technique is to predict the categorization of fresh sample points using a database wherein the data points are segregated into many different classes.

McCulloch and Pitts [27] devised an artificial neuron structure that is similar to that of a biological neuron (F).

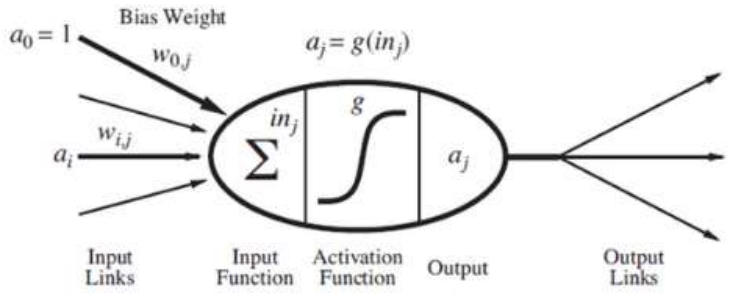

Figure 13: Mathematical Model of a single neuron [28]

There are two modules in it: the summation module Σ and the activation module F. The accumulation module is roughly equivalent to a biological nucleus. The output signal φ is formed by performing algebra summing of weighted input signals. The formula for calculating the output signal can be found here,

$$\varphi = \sum_{i=1}^{m} w_i u_i = w^T u \quad (14)$$

Where w is the weights vector (synapses comparable), u is the input signal vector (dendrites similar), and m is the number of inputs. The signal is handled by the activation module F that can be customized using various functions. The output signal y has form if a simple linear function is applied.

$$y = K \varphi \quad (15)$$

Networks that use this function are referred to as Madaline, and its neurons are referred to as Adaptive linear elements. They are the most basic networks that have found practical use. A threshold function is another sort of activation module function

$$f(x) = \begin{cases} 1, & \varphi > \varphi h \\ 0, & \varphi \leq \varphi h \end{cases} \quad (16)$$

A sigmoid function, on the other hand, describes a non-linear profile of a biological neuron more precisely when φh is a constant threshold value.

$$y = \frac{1}{1+ e^{-\beta\varphi}} \quad (17)$$

Where β is a tangensoid function and is a specified parameter

$$y = \tan h \left(\frac{\alpha\varphi}{2}\right)\frac{1- e^{-\alpha\beta}}{1+ e^{-\alpha\beta}} \quad (18)$$

Where α is the parameter that has been given. A single neuron's information capacity as well as processing ability is somewhat limited.

It can, however, be raised by the proper coupling of several neurons. Rosenblatt created the first artificial neural network, known as a perceptron, in 1958. It was used to recognise alphanumeric characters. Despite the fact that the findings were unsatisfactory, it was a success as the first system to simulate a neural network. Rosenblatt also shown that if a perceptron can solve a problem, the solution may be obtained in a finite number of steps. After nearly 15 years, research has been revived by a series of publications demonstrating that these constraints do not apply to non-linear multilayer networks. Learning strategies that are effective have also been introduced [28].

In multilayer ANNs, neurons are divided into three sorts of layers: input, output, and hidden layer. In a network, there can be one or more hidden layers, but only one output and one input layer. The type and amount of data that will be sent to the input determine the number of neurons in the input layer. The network's type of response is determined by the number of output neurons. It's more difficult to estimate the number of buried layers and their neurons. Most tasks can be solved with just one hidden layer in a network. In order to be solved, none of the known issues require a network with more than three hidden layers. Signals from the neurons in the input layer (IL) are routed to the hidden layer (HL), and then to the output layer (OL) (OL). There is no foolproof method for determining the number of hidden neurons. A formula is used to describe one of the methods.

$$N_h = \sqrt{N_i\, N_o} \quad (19)$$

Where N_i and N_o are the appropriate values for the input and output layers, correspondingly, and N_h his the number of neurons in the hidden layer. Therefore, the number of hidden neurons is normally chosen by trial and error.

5. RESULTS AND DISCUSSION

The purpose of this part is to show the numerical findings of an investigation into the secrecy rate of the proposed system, which makes use of EH for both DF and AF relaying systems. As can be seen in figure 3.5, it is assumed that the source S, the relay R, and the destination D are all situated along the same line [2], where, d_{BS}, d_{BR}, d_{SR}, d_{RE} and d_{RD} show the distance between *B* and *S*, between *B* and *R*, between *S* and *R*, between *R* and *E* and between *R* and *D*. The distance between *E* and *S* can be represented as d_{RE}=*sqrt((d_{RE})^2 + (d_{RE})^2)* respectively. The channel used is the line-of-sight (LOS) channel model $d^{\frac{-c}{2}}e^{j\theta}$, where *d* is the distance between the nodes, θ denotes the random phase that is having uniform distribution within [0,2π] and c=3.5 gives the path loss exponent [2].

It is assumed that *PB* = 30 dBm, the noise power = -40 dBm and d_{BS} = d_{BR}= 7 m. Further, α=0.999 and η = 0.9.

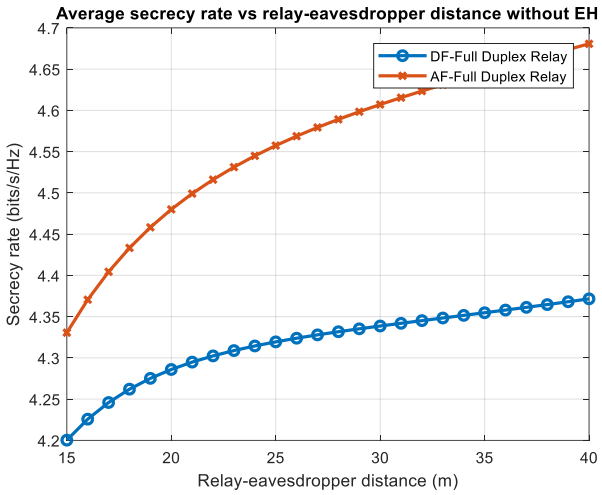

Figure 14: Secrecy rate versus Relay-eavesdropper distance (dRE)

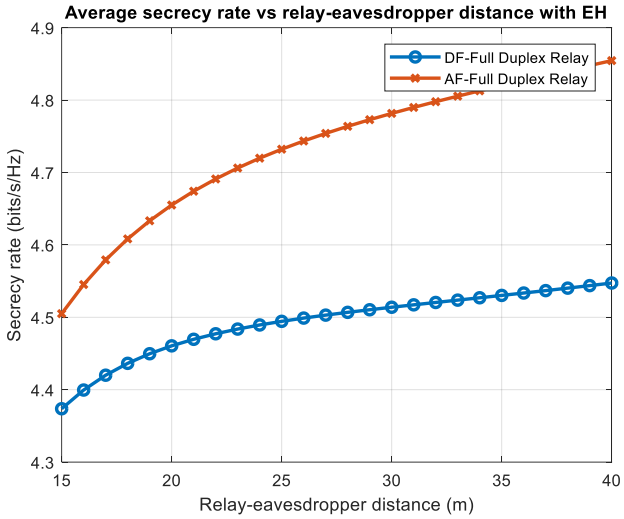

Figure 15: Secrecy rate versus Relay-eavesdropper distance (dRE) with ANN

Figures 14 and 15 show the fluctuation of secrecy rates of AF and DF cooperative strategies with the distance amongst eavesdropper and relay, dRE, when dBS = dBR = 7 metres, dSR = 10 metres, and dRD = 15 metres in the considered system that utilizes EH and in the conventional system that does not utilize EH. When there is an increase in dRE, there is also an increase in the secrecy rate, and this applies to both the DF and AF cooperative systems.

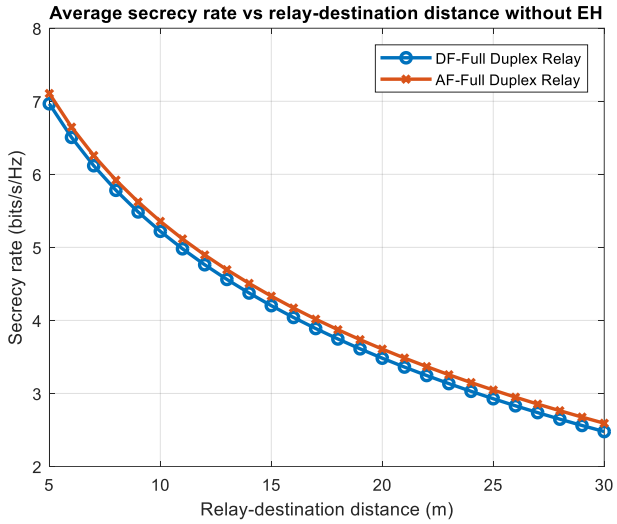

Figure 16: Secrecy rate versus Relay-destination distance (dRD)

Figures 16 and 17 show a plot of the secrecy rate versus the distance between the relay and the destination (dRD) when the relay distance (dRE) is 15 metres and the secrecy rate (dSR) is 10 metres in the proposed system with EH and in the conventional system without EH for AF and DF relaying technique, respectively. There is a decrease in the secrecy rate in both cooperative strategies whenever there is a greater distance between R and D.

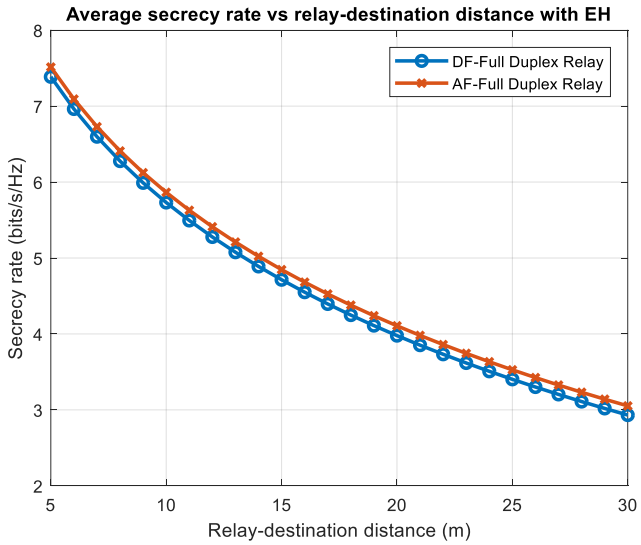

Figure 17: Secrecy rate versus Relay-destination distance (dRD) with ANN

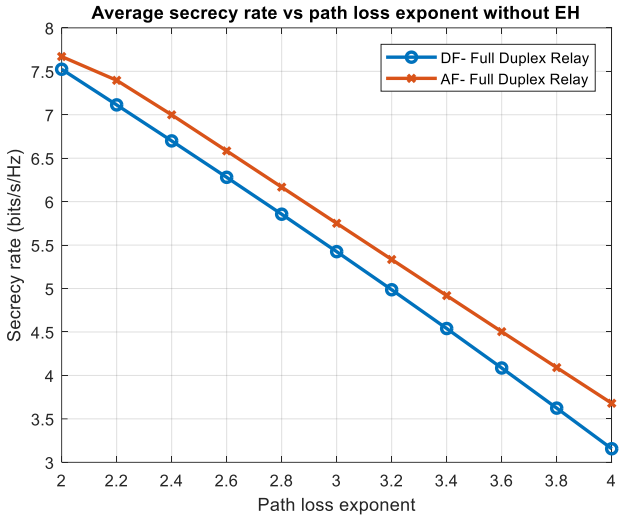

Figure 18: Secrecy rate versus Path Loss Exponent

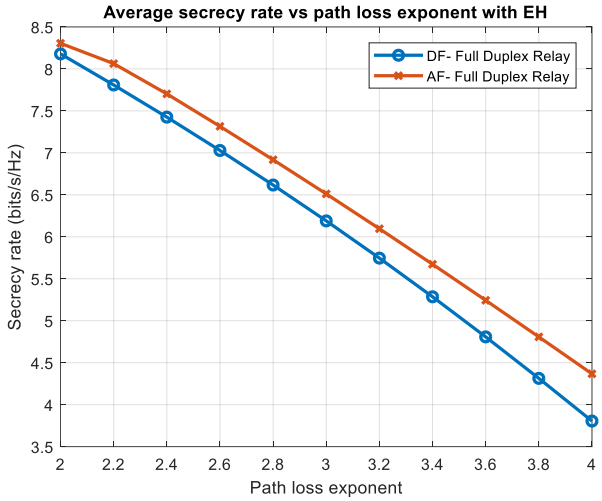

Figure 19: Secrecy rate versus Path Loss Exponent with ANN

In the proposed system, the plot of secrecy rate vs path loss exponent is depicted in figures 18 and 19 when dSR equals 10 metres, dRE equals 15 metres, dRD equals 15 metres, and dBS equals dBR equals 7 metres. When the path loss exponent is increased, the degradation of the medium is likewise increased; as a result, the secrecy rate is decreased.

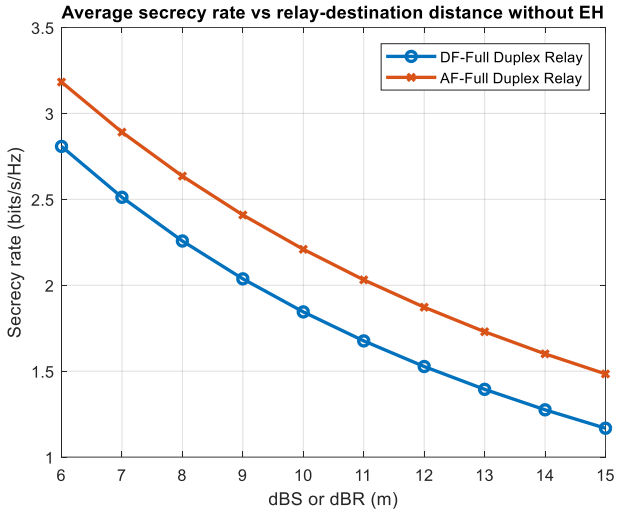

Figure 20: Secrecy rate dBS or dBR

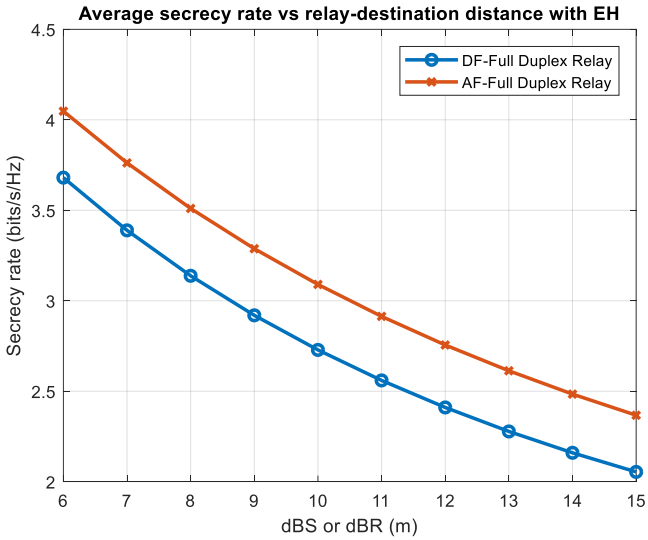

Figure 21: Secrecy rate dBS or dBR with ANN

The plot of the secrecy rate vs the distance between the beaconsource and the beacon-relay, also known as dBS or dBR, is shown in figures 20 and 21. In the proposed system, the dSR value is set to 10 metres, the dRE value is 15 metres, and the dRD value is 15 metres. The rate at which information may be kept secret is lessened whenever there is more space between a beacon and its source or relay.

7. CONCLUSION

This paper focuses on physical layer security and wireless power transmission in cooperative relaying systems for secrecy and energy harvesting. We've developed accurate mathematical equations for cooperative system analysis. These phrases simplify system analysis and evaluation. The secrecy capability of EH multiple-antennas AF relaying systems was explored when the relay used TSR and PSR to harvest energy and process information simultaneously. An generated noise signal is developed to increase relay power and system security. We developed exact analytical formulae for each EH relaying protocol's secrecy. The TSR protocol's time switching factor and PSR protocol's power splitting factor have also been tweaked to ensure the best level of anonymity across system configurations. Several critical system characteristics, including

EH time, power splitting ratio, source-to-relay distance, AN power, EH efficiency, and number of relay antennas, were also investigated.

REFERENCES

[1] H. Chen, Y. Li, J. L. Rebelatto, B. F. UchÃt'a-Filho, and B. Vucetic, "Harvest-then-cooperate: Wireless-powered cooperative communications," IEEE Transactions on Signal Processing, vol. 63, no. 7, pp. 1700–1711, April 2015.

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

[3] L. Dong, Z. Han, A. Petropulu, and H. Poor, "Improving wireless physical layer security via cooperating relays," IEEE Trans. Signal Process., vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

[4] J. Li, A. Petropulu, and S. Weber, "On cooperative relaying schemes for wireless physical layer security," IEEE Trans. Signal Process., vol. 59, no. 10, pp. 4985–4997, Oct. 2011.

[5] F.P.Fontan and P.M.Espineira, Modeling the wireless propagation channel A simulation Approach with MATLAB, 2008.

[6] J.D.Parsons, The mobile Radio Propagation Channel, 2nd ed, 2000. [16] F. T. T. P.P.Pascal Pagani and B.Uguen, Ultra-Wideband Radio Propagation Channels, 2007.

[7] H. W.-J. K. C.-C. J. Hong, Y.-W. Peter, Cooperative Communications and Networking Technologies and System Design. springer, NY, USA, 2010.

[8] T. R. W. Tranter, K. Shanmugan and K. Kosbar, Principles of Communication Systems Simulation with Wireless Applications, 1st ed. Upper Saddle River, NJ USA, 2003.

[9] G. L. Stuber, Principles of Mobile Communication, 1st ed. USA, Kluwer Academic Publishers, 1996.

[10] C. B. P. Howard Hung and S. Venkatesan, MIMO Communication for Cellular Networks. springer, NY, USA, 2012.

[11] C. B. P. H. BOLCSKEI, D. GESBERT and A.-J. V. D. VEEN, SPACE-TIME WIRELESS SYSTEMS. CAMBRIDGE UNIVERSITY PRESS, UK, 2008.

[12] M. S. John G. Proakis, Digital Communications, Fifth Edition. McGraw-Hill, NY USA, 2008.

[13] P. H. Lin and S. H. Tsai, "Performance analysis and algorithm designs for transmit antenna selection in linearly precoded multiuser mimo systems," IEEE Transactions on Vehicular Technology, vol. 61, no. 4, pp. 1698–1708, May 2012.

[14] F. Kaltenberger, M. Kountouris, D. Gesbert, and R. Knopp, "On the trade-off between feedback and capacity in measured mu-mimo channels," IEEE Transactions on Wireless Communications, vol. 8, no. 9, pp. 4866–4875, September 2009.

[15] J. Mundarath and J. Kotecha, "Optimal receive array beamforming for non-collaborative mimo space division multiple access," IEEE Transactions on Communications, vol. 58, no. 1, pp. 218–227, January 2010

[16] 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.

[17] Shannon C. E., "Communications theory of secrecy systems", The Bell System Technical Journal, vol. 28, pp. 656-715, Oct. 1949

[18] 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.

[19] Liang Y., Poor H. V., and Shamai S. "Information Theoretic Security", Delft, The Netherlands: Now Publishers, 2009.

[20] Wang Q., Xu K., and Ren K., "Cooperative secret key generation from phase estimation in narrowband fading channels", IEEE Journal on Selected Areas in Communications, vol. 30, no. 9, pp. 1666-1674, Sept. 2012.

[21] Liang Y., Poor H. V., and Shamai S. "Information Theoretic Security, ser. Foundations and Trends R in Communications and Information Theory.", Now Publishers, vol. 5, no. 4-5, 2008.

[22] Bloch M. and Barros J., "Physical-Layer Security: From Information Theory to Security Engineering", Cambridge University Press, Oct. 2011.

[23] Liu R. and Trappe W., "Securing Wireless Communications at the Physical Layer", Springer, 2010.

[24] Wen H., "Physical Layer Approaches for Securing Wireless Communication Systems", Springer Briefs in Computer Science. Springer, 2013.

[25] T. O'Shea, K. Karra, and T. C. Clancy, "Learning approximate neural estimators for wireless channel state information," in Proc. of IEEE International Workshop on Machine Learning for Signal Processing (MLSP), Tokyo, Japan, Sep. 2017.

[26] T. J. O'Shea, T. Erpek, and T. C. Clancy, "Deep learning based mimo communications," available online arXiv:1707.07980, July 2017.

[27] F. Liang, C. Shen, and F. Wu, "An iterative BP-CNN architecture for channel decoding," IEEE Journal of Selected Topics in Signal Processing, vol. 12, no. 1, pp. 144–159, Feb 2018.

[28] E. Nachmani, E. Marciano, L. Lugosch, W. J. Gross, D. Burshtein, and Y. Be'ery, "Deep learning methods for improved decoding of linear codes," IEEE Journal of Selected Topics in Signal Processing, vol. 12, no. 1, pp. 119–131, Feb 2018.

[29] Pietro Tedeschi, Savio Sciancalepore, and Roberto Di Pietro , “Security in Energy Harvesting Networks: A Survey of Current Solutions and Research Challenges”, IEEE Communications Surveys & Tutorials, DOI 10.1109/COMST.2020.3017665, Aug. 2020.

[30] Ali A. Nasir, Xiangyun Zhou, Salman Durrani, and Rodney A. Kennedy, "Relaying Protocols for Wireless Energy Harvesting and Information Processing", IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 12, NO. 7, JULY 2013.

[31] Xiao Lu, Ping Wang, Dusit Niyato, Dong In Kim, and Zhu Han, "Wireless Networks with RF Energy Harvesting: A Contemporary Survey", https://arxiv.org/abs/1406.6470v6, June 2014

[32] Yiliang Liu, Hsiao-Hwa Chen, and Liangmin Wang, "Physical Layer Security for Next Generation Wireless Networks: Theories, Technologies, and Challenges", IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. XX, MONTH YY, YEAR 2016.