Cooperative Key Establishment Protocol for Full-Duplex Relay Systems

Ali M. Allam

Department of Electronic, and Communication Engineering, Helwan University, Cairo, Egypt

***Abstract*:** Using the fading channel characteristics, as a randomness source, for the secret key generation earns significant attention because of it's computational less power and low energy consumption. Current researches focus on point-to-point reciprocal-based key extraction from these randomness sources. Most practical communication situations are non-line of sight, so endpoints use a relaying channel to improve communication performance. Besides that, in the upcoming 5G systems, the full-duplex (FD) communications will be one of the main techniques, which will remove the advantage of using the reciprocal feature in the randomness source common observation. In this paper, we consider the challenge of generating a symmetric secret key between two legitimate parties in the relaying channel with FD capability. We suggest an efficient key extraction protocol that accomplished an acceptable shared secret key rate compared to the direct channel traditional approach. Unlike similar schemes, we provide full statistical analysis for the construction of randomness source from the relaying channel with FD capability. Additionally, we investigate the performance analysis of the suggested key agreement protocol. We also analyze the effect of the curious-but-honest relay and an eavesdropper on the proposed protocol.

***Keywords*:** Key agreement, full-duplex, relaying channel, curious-but-honest relay**.**

1. Introduction

The strength of any security systems is primarily dependent on having strong keys and keeping them confidential. The key is so strong if it is difficult to guess or random. The sources of entropy that provide true randomness usually depend on physical processes or unexpected events. Recently, the construction of an entropy source based on the characteristics of fading channel has attracted significant concern [1] - [3]. The target is to establish a shared secret key with the massive rate under the constraint of no information realized from the adversary's observation regarding the secure key. Since the channel state varies, instantaneous channel state information (CSI) needs to be estimated on a short-term basis, employing a conventional approach training sequence (or pilot sequence). Therefore, it is obvious to detect that the first stage in key extraction from wireless channel conditions is channel estimation. The second step is the quantization, which is the response of converting the common observation to a string of binary bit sequences. A longer length of the derived bit sequence with high entropy is the principal goal of the quantization step. Information reconciliation is the next step, where the mismatch between the bit strings at two parties due to many factors, such as noise, interference, and the time lag between transmission and reception, is detected and corrected applying an interactive error detection and correction algorithm employing a public channel message exchange. The last stage represented by privacy amplification where it uses a hashing mechanism. Privacy amplification has two important functions. First, decreasing the information leaked from the previous step. Second, use the arbitrary input from the previous stage to generate a fixed output fit for practice as a secret key for a standard encryption algorithm as AES which uses 128-bit string. These four stages formed the tools employed for the key generation from physical layer characteristic [4] - [5].

Channel estimation training mechanism is the only method, as in most of the previous works [6]-[7], to allow legitimate endpoints to commonly observe a randomness source without the need for any key distribution infrastructure, which is the advantage of this method over the traditional cryptographic-based key distribution [8]-[9]. Besides that, this method has no computation power and low energy consumption [10]. In most of the previous works, the key generation suggested schemes exploited the reciprocity feature of the channel gain in time-duplex TD systems, besides that the assumption of a direct connection between endpoints.

In the upcoming 5G systems, one of the essential technologies is the full-duplex communication. In the FD system, each pair of node communicates over two different bands, one for transmission, and another for receiving signals, simultaneously. So each link between two nodes composite of two paths, with two different channel state, between them. The problem of secret key generation, between two nodes in FD systems, is more complicated due to the non-reciprocity of the channel gains between the two nodes.

The indirect connection between two nodes has solved by using relays [11] to improve the performance and coverage of wireless networks. The overall channel from the source to the destination via the relay, in amplifying and forwarding (A & F) systems, is two Gaussian channels with features considerably different from a typical cellular channel [12].

In our novel work [13], we developed a key extraction protocol based on the non-reciprocity of FD channel. As a result, one can design a scheme that can exploit the randomness provided by round-trip FD link between two terminals. In this paper, we exploit this fact and extend our work in [13] to the case of cooperation communication systems. In this paper, we regard the channel estimation stage, of key extraction from FD relay channel, to prove the feasibility of establishing a common randomness source based on the FD wireless relaying channel. Besides that, we measure the amount of entropy resulting from that source and determine if it is suitable for a secret key generation between two nodes. We briefly discuss the simulation of randomness source based on the relay fading channel and verify our theoretical results via simulations. To the best of our knowledge, this is the first consideration for the construction of randomness source based on an overall round-trip relay fading channels in FD systems. In this subsection, we inspect former works in relaying-based key

generation schemes. A common theme in most of this work is the selection of the reciprocity characteristic of a fading channel to achieve a common observation between parties to share a randomness source.

Popular cooperative-based key generation scheme usually applies time duplex relay, because of simple observation for a common source. For instance, in [14] presented a two-way half-duplex relaying system composed of two legitimate nodes try to establish a shared secret key with the aid of a relay. The schemes suggested exploiting the fading channel coefficients between each pair of nodes in the system model to construct a random source composed of the product of two fading channel gains. In [15], the authors scrutinized the technique followed in [14] to generate a secret key. Their criticism summarized as follows: 1) the rate reduction of the resultant secret key due to the leakage of information about the channel gain to the eavesdropper was because the relay re-sent the received signal, which contains the information about the channel gain. 2) The challenge to assess the secret key rates of the schemes proposed in [14]. Because of the probability density function (pdf) of the estimated virtual channel gain, the product of two physical channel gains is complicated.

To avoid the challenge of estimating the rate of the secret key for schemes in [14], and improve its performance. The authors presented, in [15], a key generation scheme for bidirectional relay channel between two nodes. In this scheme, they are exploiting the reciprocity feature of fading channel between each pair of nodes to generate two keys, one between the first node with the relay and the other with the second node with the relay, and then the relay broadcast the XORing of the resultant two keys. The suggested scheme in [15] was depending on the reciprocity feature of fading channel, and at the same time, there is no determination of the role of the two legitimate nodes, i.e., the initiator and the responder. The connection of the two nodes by the relay causes the use of that protocol in an actual situation not effective because the establishment of this connection wastes the communication resources of the system.

In [16], the authors proposed a pilot- based channel estimation approach of a feedback system to estimate a virtual channel gain, which composed of a combination of the channel gain of two paths in a point-to-point FD system, and employed it as a common randomness source between two parties to generate a shared secret key. However, as followed in [14], the authors did not estimate the key rate of the suggested scheme due to the complexity of the resulted pdf of the virtual channel gain.

In [17], the authors examined the key generation difficulty for an FD relay channel. In [17], they avoid the challenge of evaluating the pdf of the product of the channel gains by using the reciprocity feature of the channel fading gain and use the FD capability for the relay to communicate with the two nodes at the same time.

In the context of prior efforts in a relay-based key generation, it is evident that estimating the probability density function of the product of the channel gains, to measure the performance of the designed protocol in term of the secret key rate, is an open problem. We attempt to accept this challenge in this work.

In this article, we examine a significant practical communication scenario in FDD systems. The suggested scenario composed of two legitimate nodes with no direct connection and an untrusted relay aided them for communication. In this paper, we establish a secure channel between two nodes by generating a secret key from a common observation of FD relaying channel-based randomness source, in the presence of an eavesdropper and with the cooperation of untrusted relay. A novel randomness source constructed based on the FD relaying system, besides the measuring of the performance of the system. Numerical results corresponding to theoretical analysis will also provide. The contributions of this paper can be summarized as follows:

- Construct a randomness source composed of four cascaded FD fading channels.
- Suggest a scheme based on round-trip training mechanism to provide a common observation of the constructed randomness source for the two endpoints in the elimination of channel reciprocity feature due to the FD system.
- Finding the entropy of the random source and compare it with the traditional single-channel gain based randomness source.
- We analyze the effect of an untrusted relay and an eavesdropper on the performance of our submitted scheme.

We have organized the rest of this paper in the following way. Section 2 describes the system model under investigation and provides the assumption necessary for our suggested schemes. In section 3, we present the establishment of an FD relay channel-based randomness source. We propose a secret key generation protocol, in the presence of an adversary, and determine its secret key rate in sections 4. Numerical results presented in section 5; finally, concluding notes are provided in section 6.

2. System Model

The purpose of this section is to introduce the communication model and the hypothesis held in this paper. Fig. 1 shows the conventional model of the bidirectional relaying system that forms of four parties, two legitimate nodes (an initiator (node A), and a responder (node B)), an honest-but-curious relay (node R), and a passive attacker (node E). Node A needs to establish a secure channel with node B with the cooperation of node R, due to the absence of a direct channel between node A and node B, in the presence of node E. The relay role will be amplify-and-forward the message from node A to node B but may try to get any information about the generated secret key. Node E is an eavesdropper, who monitors the messages between the other parties without interfering or modification. All the terminals in the model are using FD communication, except node E that is receiving node only (inactive adversary).

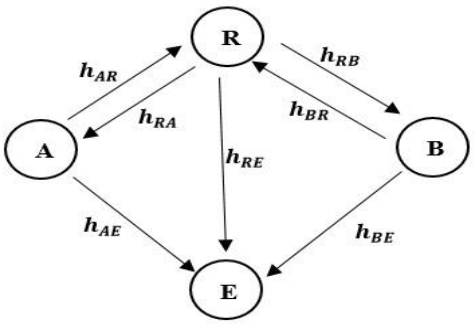

Figure 1. System Model

In precise, when node A sends a private probe signal X_A during a given channel use, node R and node E will receive,

$$Y_R = h_{AR}X_A + N_R \quad (1)$$
$$Y_E = h_{AE}X_A + N_E \quad (2)$$

respectively, where h_{AR} is the fading channel gain for the path between node A and node R, N_R is zero mean univariate normal distribution noise with variance σ^2 at node R , h_{AE} is the fading coefficient from node A to node E, N_E is the noise at node E.

Identically, when node B forwards a private probe signal X_B during a given channel use, node R and node E will get,

$$Y_R = h_{BR}X_B + N_R \quad (3)$$
$$Y_E = h_{BE}X_B + N_E \quad (4)$$

respectively, where h_{BR} is the fading channel gain for the path between node B and node R, h_{BE} is the fading coefficient from node B to node E. For briefing, the signal model for node R is similar.

We follow the same assumption held in this field of research [18]-[20], which list as follow;

- All the fading coefficients in the system model, summarized in table 1, are assumed to be zero mean univariate normal distribution with variances,

Table 1: variances assigned to channel gains

h_{AR}	h_{RB}	h_{BR}	h_{RA}
σ_1^2	σ_2^2	σ_3^2	σ_4^2

- The noise at any node is zero mean univariate normal distribution with variance σ^2.
- All channel gains and noises in the system are random variables and independent of each other.
- No member of the system knows the value of any fading coefficient a priori, but all members of the system identify its statistical distribution.
- The noise in all channels independently and identically distributed.

In this paper, we consider the FD communication mode, which means that the channels are non-reciprocal, i.e., $h_{AR} \neq h_{RA}$. Furthermore, we consider an ergodic block-fading model for the wireless channel, which means that the channel gain remains constant for a period of T symbols and changes randomly to another independent value after the current period [21].

For each node, let $X_n = [x_n(1), \dots, x_n(L_n)]'$ represent the signals sent by node $n \in \{A, B, R\}$ in L_n the channel uses. As in [19], we suppose that the transmitted power constraint for each terminal is equal, for simplicity, i.e.,

$$\frac{1}{L_n}\mathbb{E}\{X_n' X_n\} \leq P_T, \forall\, n \in \{A, B, R\} \quad (5)$$

3. Common Randomness Source Construction

In this section, we construct a novel randomness source, which can be commonly observed by legitimate nodes to generate a secret key. In channel reciprocal-based key extraction, the randomness source mainly established from the fading channel gain of the point-to-point connection between two legitimate terminals. The two users can commonly observe this randomness source by using the traditional training technique. The observation process is straightforward due to the reciprocity feature of the fading channel between two users in time duplex (TD) system. This entropy source employed in most of the research of key extraction based on channel status information (CSI) [18]-[20].

In our scenario, we have two different situations than most of the communication scenarios taken into consideration in the previous related works. First, we have no direct connection between node A and node B. Second, we consider FD communication systems. In our case of relaying FD system, the link between two legitimate nodes (node A and B) composed of four paths with four different channel gains h_{AR} , h_{RB}, h_{BR} and h_{RA} as shown in figure 1. That occurs due to the use of different frequencies for communication between each pair of nodes in both directions (forward and reverse). To establish a randomness source for this communication scenario, we have to use the idea of cascaded channel gains of the four paths to produce an overall fading channel gain for the link $h = h_{AR}h_{RB}h_{BR}h_{RA}$. The product operation arises from the treatment of the whole link as it is composed of four paths in cascaded. In this case, the way to make both nodes get the same observation is using a round-trip training strategy discussed in the next section.

The challenge of using the suggested randomness source is how to asset its performance. In [15], the authors stated that it is difficult to estimate the secret key rate of a key generation system based on composite two fading channel gains because of the unavailability of the probability density function of that randomness source. From this article, no study attempts to solve this open problem on our knowledge.

In this paper, we try to accept this challenge, to compute the uncertainty of the randomness source, which comprised of four-cascaded fading channel gain and compares it with the one composed of only one channel gain (the reciprocity case).

We need to measure the uncertainty for both randomness sources used in the key extraction and compare the performance of each source. The uncertainty of a source measured by differential entropy $h(x)$, as in [22], the differential entropy of a univariate normal distribution with variance σ_0^2 is,

$$h(x) = \frac{1}{2}\log(2\pi e\sigma_0^2) \quad (6)$$

Theorem 1: the overall channel gain h of the link between node A and node B has a zero mean Gaussian distribution with variance $\frac{\sigma_x^2\sigma_y^2}{(\sigma_x^2+\sigma_y^2)^2}$, Where, $\sigma_x^2 = \frac{\sigma_1^2\sigma_2^2}{(\sigma_1^2+\sigma_2^2)^2}$ and $\sigma_y^2 = \frac{\sigma_3^2\sigma_4^2}{(\sigma_3^2+\sigma_4^2)^2}$.

Proof:

We need to compute the variance of the overall channel gain, $h = h_{AR}h_{RB}h_{BR}h_{RA}$. To compute the amount of entropy of the constructed randomness source.

Since the four channel state h_{AR} , h_{RB}, h_{BR} and h_{RA} are assumed to be a zero mean univariate normal distribution with variance σ_1^2 , σ_2^2, σ_3^2 and σ_4^2, respectively.

As shown in [23], the product, of two Gaussian random variables, is a scaled Gaussian distribution, and the scale is Gaussian.

So, the Product of two Gaussians pdfs, $h_{AR} \sim \mathcal{N}(\mu_1, \sigma_1^2)$, and $h_{RB} \sim \mathcal{N}(\mu_2, \sigma_2^2)$is:

$$h_{AR}\,h_{RB} = \frac{S_x}{\sqrt{2\pi\sigma_x^2}} \exp\left[-\frac{(x-\mu_x)^2}{2\sigma_x^2}\right] \quad (7)$$

where,

$\sigma_x^2 = \frac{\sigma_1^2\sigma_2^2}{\sigma_1^2+\sigma_2^2}$, and $\mu_x = \frac{\mu_1\sigma_2^2+\mu_2\sigma_1^2}{\sigma_1^2+\sigma_2^2}$

$$S_x = \frac{1}{\sqrt{2\pi(\sigma_1^2+\sigma_2^2)}} \exp\left[-\frac{(\mu_1-\mu_2)^2}{2(\sigma_1^2+\sigma_2^2)}\right] \quad (8)$$

Under our assumption, we have zero mean in all the random variable distributions. Then,

$\mu_x = 0$ and $S_x = \frac{1}{\sqrt{2\pi\left(\sigma_{ij}^2+\sigma_{ji}^2\right)}}$

For any $X_a \sim \mathcal{N}(\mu_a,\sigma_a^2)$, $cX_a = \mathcal{N}(c\mu_a,c^2\sigma_a^2)$, scaling of the normal distribution.

So,

$$h_{AR}\,h_{RB} \sim \mathcal{N}\left(0,\frac{\sigma_1^2\sigma_2^2}{(\sigma_1^2+\sigma_2^2)^2}\right) \quad (9)$$

Similar,

$$h_{BR}\,h_{RA} \sim \mathcal{N}\left(0,\frac{\sigma_3^2\sigma_4^2}{(\sigma_3^2+\sigma_4^2)^2}\right) \quad (10)$$

So,

$$h = h_{AR}\,h_{RB}\,h_{BR}\,h_{RA} \sim \mathcal{N}\left(0,\frac{\sigma_x^2\sigma_y^2}{(\sigma_x^2+\sigma_y^2)^2}\right) \quad (11)$$

$$Var(h) = \frac{\sigma_x^2\sigma_y^2}{(\sigma_x^2+\sigma_y^2)^2} \quad (12)$$

Where,

$$\sigma_x^2 = \frac{\sigma_1^2\sigma_2^2}{(\sigma_1^2+\sigma_2^2)^2} \quad (13)$$

$$\sigma_y^2 = \frac{\sigma_3^2\sigma_4^2}{(\sigma_3^2+\sigma_4^2)^2} \quad \blacksquare(14)$$

So, the uncertainty of four cascaded fading channel gains, $h_{AR}\,h_{RB}\,h_{BR}\,h_{RA}$ is,

$$h(x) = \frac{1}{2}\log(2\pi e\ var(h)) \quad (15)$$

If we assume that, all the fading channel gains have equal variances. So,

$$h(x) = \frac{1}{2}\log_2\left(\frac{\pi}{2}\ e\right) \quad (16)$$

The amount of uncertainty, in the randomness source composed of four cascaded fading channel gains, is constant and can be controlled by the amount of amplification of the relay.

Next, we are going to show how to share the randomness source between two parties in the presence of adversary attacker and the help of curious-but-honest relay.

4. Key Establishment Protocol

In this section, we examine the secret key generation problem in the full-duplex relaying channel system. Firstly, we explain the scheme of a secret key agreement between two terminals; have no direct connection between each other, employing a relay for connection, and the presence of a passive eavesdropper. We then introduce the security analysis corresponding to the suggested scheme. Finally, we exam the performance of the suggested scheme in the construction of the secret key rate.

4.1 Suggested Protocol

The system model for the proposed protocol shown in figure1. Node A and node B decide to commonly observe the randomness source presented in the previous section by applying the training technique for establishing a secret key. The corresponding channel use of the scheme shown in figure 2, the transmission organized in cycles of duration T time slot each. The time frame structure for one cycle shown in the figure.

← T →					
A sends to R	R sends to B	B sends to R	R sends to A	A sends to R	R sends to B
$\leftarrow T/8\rightarrow$	$\leftarrow T/8\rightarrow$	$\leftarrow T/4\rightarrow$	$\leftarrow T/4\rightarrow$	$\leftarrow T/8\rightarrow$	$\leftarrow T/8\rightarrow$

Figure 2: Time frame for the suggested protocol

The training stage is done in a sequential fashion, because of the round-trip nature of the training signal, started from node A to node B via node R and ended from node B to node A via node R. We assume that the transmission duration is $T/8$ for one signal transmission.

The initiator (node A) intends to establish a secure channel with the responder (node B) through a relay (node R) due to the non-line of sight between initiator and responder. For this purpose, both nodes (A and B) use a private probe signal X_A and X_B respectively, for two reasons: improving the security of the secret key establishment protocol, by reducing the information leakage from transmitted signals. 2) Using it in round-trip training technique to estimate the overall channel status ($h_{AR}\,h_{RB}\,h_{BR}\,h_{RA}$), due to the non-reciprocity feature of FD link. Subsequent, both nodes can generate a shared secret key from the common observation of the round-trip training sequences. We now describe the steps of the scheme in more detail.

Step 1:

Node A employs the channel for a duration $\frac{T}{8}$ to send a private probe signal X_A. Node R receives,

$$Y_{R1} = h_{AR}X_A + N_R \quad (17)$$

In addition, node E intercepts,

$$Y_{E1} = h_{AE}X_A + N_E \quad (18)$$

Step 2:

Node R amplifies and forwards Y_{R1} to node B during $\frac{T}{8}$ of the fading block T. Node B gets,

$$Y_{B2} = h_{RB}Y_{R1} + N_B \quad (19)$$

We assume a unity amplification by the relay to any signal for simplicity. So,

$$Y_{B2} = h_{RB}h_{AR}X_A + h_{RB}N_R + N_B \quad (20)$$

Again, node E intercepts,

$$Y_{E2} = h_{RE}Y_{R1} + N_E \quad (21)$$

$$Y_{E2} = h_{RE}h_{AR}X_A + h_{RE}N_R + N_E \quad (22)$$

Step 3:

Now, the responder (node B) has to finish the round-trip training sequence originated by node A, and want to rise a new round-trip training sequence for his observation of the common randomness source. So, node B has to send two signals during $\frac{T}{4}$, sequentially one for node A's training sequence and the other for his training sequence. So he sends Y_{B2}, and a private probe X_B to node R. Node R receives,

$$Y_{R31} = h_{BR}X_B + N_R \quad (23)$$

$$Y_{R32} = h_{BR}Y_{B2} + N_R \quad (24)$$

$$Y_{R32} = h_{BR}h_{RB}h_{AR}X_A + h_{BR}h_{RB}N_R + h_{BR}N_B + N_R \quad (25)$$

In addition, node E intercepts,

$$Y_{E31} = h_{BE}X_B + N_E \quad (26)$$

$$Y_{E32} = h_{BE}Y_{B2} + N_E \quad (27)$$

$$Y_{E32} = h_{BE}h_{RB}h_{AR}X_A + h_{BE}h_{RB}N_R + h_{BE}N_B + N_E \quad (28)$$

Step 4:
Node R honestly amplify and forward the received signals from node B. Node A gets both,

$$Y_{A41} = h_{RA}Y_{R31} + N_A \quad (29)$$
$$Y_{A42} = h_{RA}Y_{R32} + N_A \quad (30)$$

Where,

$$Y_{A41} = h_{RA}h_{BR}X_B + h_{RA}N_R + N_A \quad (31)$$
$$Y_{A42} = h_{RA}h_{BR}h_{RB}h_{AR}X_A + h_{RA}h_{BR}h_{RB}N_R + h_{RA}h_{BR}N_B + h_{RA}N_R + N_A \quad (32)$$

Besides that, node E intercepts,

$$Y_{E41} = h_{RE}Y_{R31} + N_E \quad (33)$$
$$Y_{E42} = h_{RE}Y_{R32} + N_E \quad (34)$$

Where,

$$Y_{E41} = h_{RE}h_{BR}X_B + h_{RE}N_R + N_E \quad (35)$$
$$Y_{E42} = h_{RE}h_{BR}h_{RB}h_{AR}X_A + h_{RE}h_{BR}h_{RB}N_R + h_{RE}h_{BR}N_B + h_{RE}N_R + N_E \quad (36)$$

Step 5:
Node A will send Y_{A41} to node B via node R. The relay receives,

$$Y_{R5} = h_{AR}Y_{A41} + N_R \quad (37)$$
$$Y_{R5} = h_{AR}h_{RA}h_{BR}X_B + h_{AR}h_{RA}N_R + h_{AR}N_A + N_R \quad (38)$$

In addition, node E receives,

$$Y_{E5} = h_{AE}Y_{A41} + N_E \quad (39)$$
$$Y_{E5} = h_{AE}h_{RA}h_{BR}X_B + h_{AE}h_{RA}N_R + h_{AE}N_A + N_E \quad (40)$$

Step 6:
The relay sends Y_{R5} to node B, that receives,

$$Y_{B6} = h_{RB}Y_{R5} + N_B \quad (41)$$
$$Y_{B6} = h_{RB}h_{AR}h_{RA}h_{BR}X_B + h_{RB}h_{AR}h_{RA}N_R + h_{RB}h_{AR}N_A + h_{RB}N_R + N_R \quad (42)$$

In addition, node E receives,

$$Y_{E6} = h_{RE}Y_{R5} + N_E \quad (43)$$
$$Y_{E6} = h_{RE}h_{AR}h_{RA}h_{BR}X_B + h_{RE}h_{AR}h_{RA}N_R + h_{RE}h_{AR}N_A + h_{RE}N_R + N_E \quad (44)$$

At the end, node A and node B have a common observation for overall channel status $h_{AR}h_{RB}h_{BR}h_{RA}$ from Y_{A42} and Y_{B6}. The overall channel gain of the relaying system is

$$h = h_{AR}h_{RB}h_{BR}h_{RA} \quad (45)$$

At the end of our protocol, node A figure out a noisy estimation of the overall channel gain of the relaying system $\tilde{h}_A$ from Y_{A42}, as follow,

$$\tilde{h}_A = \frac{x_A^T}{\|x_A\|^2}Y_{A42} \quad (46)$$
$$\tilde{h}_A = h_{AR}h_{RB}h_{BR}h_{RA} + h_{RA}h_{BR}h_{RB}\frac{x_A^T}{\|x_A\|^2}N_R + h_{RA}h_{BR}\frac{x_A^T}{\|x_A\|^2}N_B + h_{RA}\frac{x_A^T}{\|x_A\|^2}N_R + \frac{x_A^T}{\|x_A\|^2}N_A \quad (47)$$

in which $\|\cdot\|$ signifies the norm of its argument. Also, node B figure out $\tilde{h}_B$ from Y_{B6} through

$$\tilde{h}_B = \frac{x_B^T}{\|x_B\|^2}Y_{B6} \quad (48)$$
$$\tilde{h}_B = h_{AR}h_{RB}h_{BR}h_{RA} + h_{RB}h_{AR}h_{RA}\frac{x_B^T}{\|x_B\|^2}N_R + h_{RB}h_{AR}\frac{x_B^T}{\|x_B\|^2}N_A + h_{RB}\frac{x_B^T}{\|x_B\|^2}N_R + \frac{x_B^T}{\|x_B\|^2}N_B \quad (49)$$

where, $\|X_A\|^2$ and $\|X_B\|^2$ are the energy of each training sequence. We assume that the relay is in the midway between node A and node B. In addition, the total power constraint is equivalent to,

$$\frac{1}{3}(P_A + P_B + P_R) \le P_T \quad (50)$$

So, the energy of each training sequence is equally due to the assumption of placement of the relay and the fair use of the channel during the training phase.

$$\|S\|^2 = \|S_A\|^2 = \|S_B\|^2 = \|S_R\|^2 = TP_T/8 \quad (51)$$

We use h to denote $h_{AR}h_{RB}h_{BR}h_{RA}$, ξ_1 to denote $h_{RA}h_{BR}h_{RB}\frac{x_A^T}{\|x_A\|^2}N_R$, ξ_2 to denote $h_{RA}h_{BR}\frac{x_A^T}{\|x_A\|^2}N_B$, ξ_3 to denote $h_{RA}\frac{x_A^T}{\|x_A\|^2}N_R$, and ξ_4 to denote $\frac{x_A^T}{\|x_A\|^2}N_A$. Hence, (47) can be rewritten as

$$\tilde{h}_A = h + \xi_1 + \xi_2 + \xi_3 + \xi_4 \quad (52)$$

Also, we use Γ_1 to denote $h_{RB}h_{AR}h_{RA}\frac{x_B^T}{\|x_B\|^2}N_R$, Γ_2 to denote $h_{RB}h_{AR}\frac{x_B^T}{\|x_B\|^2}N_A$, Γ_3 to denote $h_{RB}\frac{x_B^T}{\|x_B\|^2}N_R$ and Γ_4 to denote $\frac{x_B^T}{\|x_B\|^2}N_B$. Hence, (49) can be rewritten as,

$$\tilde{h}_B = h + \Gamma_1 + \Gamma_2 + \Gamma_3 + \Gamma_4 \quad (53)$$

The first term in equation (52) and (53) represents the overall channel gain of the link between node A and node B (Common Randomness Source). The other terms, in the observation, describe the noise that disturbs the observation and cause estimation error in the channel state information.

4.2 Security Analysis

In this paper, we will consider the eavesdropping attacks from both honest-but-curious relay and an eavesdropper. Relay node can only launch passive attacks. In other words, the relay node would obey with the transmission protocol; however, it is curious about the messages from the users and tries to recover them, i.e., referred to an honest-but-curious adversary model. Before computing the secret key rate of suggested key established protocol, we will provide the security analysis of the suggested scheme to quantify the amount of information leakage about h during the protocol messages exchange. Therefore, we will figure, in the next subsection, the secret key rate of our protocol.

According to the secret key capacity of a secret key generated in the presence of adversary introduced by Maurer [24]. The secret key capacity generated between node A and node B, in the presence of an adversary and curious relay, denoted by $S(\tilde{h}_A; \tilde{h}_B \| \tilde{h}_{E4}, \tilde{h}_{R3})$. It defined as the maximum of all possible secret key rates. According to [25], the secret key capacity between two nodes specified as follows,

$$S(\tilde{h}_A; \tilde{h}_B \| \tilde{h}_{E4}, \tilde{h}_{R3}) = I(\tilde{h}_A; \tilde{h}_B | \tilde{h}_{E4}, \tilde{h}_{R3}) \quad (54)$$

That means the generated secret key capacity depends on the mutual information of the common observation between node A and node B, besides the amount of information the adversary and the relay recognize. This leakage of information to the adversary and relay came from the round-trip training method used by the two legitimate users to establish a common observation for the randomness source.

If we considered a passive opponent, then $\tilde{h}_A$ and $\tilde{h}_B$ are jointly univariate normal random variables, because of the independence of all noises and channel gains in our system model. Node A and node B will establish a key from these two correlated observations. As will be express in consequence, our scheme will establish a key from $(\tilde{h}_A, \tilde{h}_B)$ with a rate,

$$R_S = \frac{1}{T} I(\tilde{h}_A; \tilde{h}_B | \tilde{h}_{E4}, \tilde{h}_{R3}) \quad (55)$$

That is the amount of uncertainty shared by both nodes from the observation of the randomness source during a coherence time T (before the change of the condition of the channel).

$$R_S = \frac{1}{T}\left[I(\tilde{h}_A; \tilde{h}_B) - I(\tilde{h}_A; \tilde{h}_{E4}, \tilde{h}_{R3})\right]^+ \quad (56)$$

where $[x]^+ = max\{0, x\}$, because the value of the rate must be positive. The normalization factor $\frac{1}{T}$ is due to the changing of channel characteristics every T sequence time, i.e., the link channel gains between the parties remain consists only for a block of T sequence times. Generally, $I(\tilde{h}_A; \tilde{h}_B)$ is the common randomness that both node A and node B share, and $I(\tilde{h}_A; \tilde{h}_{E4}, \tilde{h}_{R3})$ is the quantity of information that the adversary and relay recognize about the value of $\tilde{h}_A$.

Therefore, by computing $I(\tilde{h}_A; \tilde{h}_{E4}, \tilde{h}_{R3})$, we can quantify the amount of leaking information.

$$I(\tilde{h}_A; \tilde{h}_{E4}, \tilde{h}_{R3}) = h(\tilde{h}_A) - h(\tilde{h}_A | \tilde{h}_{E4}, \tilde{h}_{R3}) \quad (57)$$

Where, $h(\cdot)$ is the differential entropy of its argument. Assuming that, all channel coefficients and noise are independent. So,

$$h(\tilde{h}_A | \tilde{h}_{E4}, \tilde{h}_{R3}) = h(\tilde{h}_A) \quad (58)$$

From equation (58), we can deduce that our protocol leakage no information about the secret key to node R and node E.

4.3 Key Generation Rate

The performance of our suggested protocol measured in term of secret key rate R_S. In this subsection, we determine the secret key rate of our protocol. Since,

$$R_S = \frac{1}{T} I(\tilde{h}_A; \tilde{h}_B | \tilde{h}_{E4}, \tilde{h}_{R3}) \quad (59)$$

$$R_S = \frac{1}{T}\left[I(\tilde{h}_A; \tilde{h}_B) - I(\tilde{h}_A; \tilde{h}_{E4}, \tilde{h}_{R3})\right]^+ \quad (60)$$

We will estimate the secret key rate regarding node A, which is the same for node B. We can rewrite R_S as follows:

$$TR_S = I(\tilde{h}_A; \tilde{h}_B) - I(\tilde{h}_A; \tilde{h}_{E4}, \tilde{h}_{R3}) \quad (61)$$

$$= h(\tilde{h}_A) - h(\tilde{h}_A | h_B) - h(\tilde{h}_A) + h(\tilde{h}_A | \tilde{h}_{E4}, \tilde{h}_{R3}) \quad (62)$$

$$= h(\tilde{h}_A | \tilde{h}_{E4}, \tilde{h}_{R3}) - h(\tilde{h}_A | \tilde{h}_B) \quad (63)$$

Since all channel gains are statistically independent. So,

$$= h(\tilde{h}_A) - h(\tilde{h}_A | \tilde{h}_B) \quad (64)$$

According to [26], we have,

$$h(\tilde{h}_A | \tilde{h}_B) = h(\tilde{h}_A - c\tilde{h}_B | \tilde{h}_B) \quad (65)$$

$$\leq h(\tilde{h}_A - c\tilde{h}_B) \quad (66)$$

Since, $(\tilde{h}_A, \tilde{h}_B)$ are jointly Gaussian, and if we choose,

$$c = cov(\tilde{h}_A, \tilde{h}_B) / var(\tilde{h}_B) \quad (67)$$

then, $(\tilde{h}_A - c\tilde{h}_B)$ and $\tilde{h}_B$ are independent, and the upper bound for $h(\tilde{h}_A | \tilde{h}_B)$ is,

$$h(\tilde{h}_A | \tilde{h}_B) = h(\tilde{h}_A - c\tilde{h}_B) \quad (68)$$

Since,

$$c\tilde{h}_B \sim \mathcal{N}(0, c^2 var(\tilde{h}_B)) \quad (69)$$

$$\sim \mathcal{N}\left(0, \left(cov(\tilde{h}_A, \tilde{h}_B)\right)^2 / var(\tilde{h}_B)\right) \quad (70)$$

So,

$$R_S = \frac{1}{T}\left[h(\tilde{h}_A) - h(\tilde{h}_A - c\tilde{h}_B)\right] \quad (71)$$

$$R_S = \frac{1}{T} h(c\tilde{h}_B) \quad (72)$$

$$R_S = \frac{1}{2T} \log\left(2\pi e \left(cov(\tilde{h}_A, \tilde{h}_B)\right)^2 / var(\tilde{h}_B)\right) \quad (73)$$

Where,

$$COV(\tilde{h}_A; \tilde{h}_B) = var(h) \quad (74)$$

$$var(\tilde{h}_B) = var(h) + var(\Gamma_1) + var(\Gamma_2) + var(\Gamma_3) + var(\Gamma_4) \quad (75)$$

We can estimate the variance of $\Gamma_1, \Gamma_2, \Gamma_3$, and Γ_4, if we consider theorem 1. The rate shows that the entropy of the observation reduced due to the effect of the noise that disturbs the observation.

5. Simulation Analysis

From the secret key rate formulate that derived in the previous section; we can deduce the parameters affect the rate as follow:

- Coherence duration.
- Transmitted power constraint.
- Channel gains and noise.

In this section, we show various simulation results to illustrate the performance of our suggested scheme and show the effect of each parameter on the secret key rate. Besides that, we compare the performance of our scheme with the schemes presented by Takayki et al.[14] (as TD relaying channel based key extraction protocol), and Lai et al.[15] (as reciprocity based key extraction scheme). We follow the same values of the parameters as most of the papers in this field [18]-[20]. The value of the simulation parameters summarized in table 2.

Table 2. Value of the simulation parameters

Parameter	T	σ_1^2	σ_2^2	σ_3^2	σ_4^2	σ^2
Value	99	0.1	0.2	0.3	0.4	0.1

Initial, we measured the performance of our new randomness source, which composed of four fading channels in term of entropy. Figure 3 showed that the entropy measure of our randomness source is constant regardless of the amount of the individual gain for each fading channel. This remarkable result holds due to the mathematical analysis in the previous section, the significance of this result is the independence of the amount of the randomness source of the channel gain, which is poor in the wireless systems. Besides that, the amount of entropy can increase if we put relay amplification factor in consideration. In addition, the figure showed that the advantage of our source in case of poor channel condition, i.e., less than 0.25.

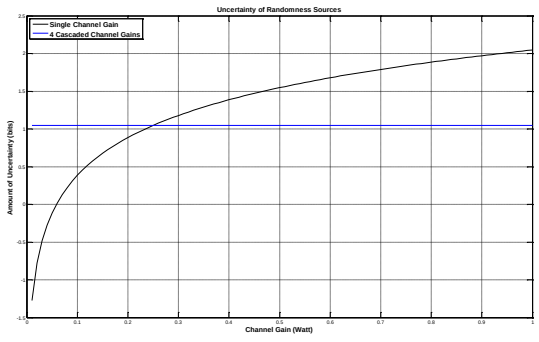

Figure 3: Comparison of the uncertainty of random sources

In figure 4, we held a comparison between our suggested protocol and two other schemes designed for the same purpose and discussed in the related work subsection. The figure shows the relation between the key generation rate and the transmitted power. As shown the key rate resulting from

a single fading channel based randomness source is the smallest and the key rate depending on relaying system is bigger whatever the value of the transmitted signal.

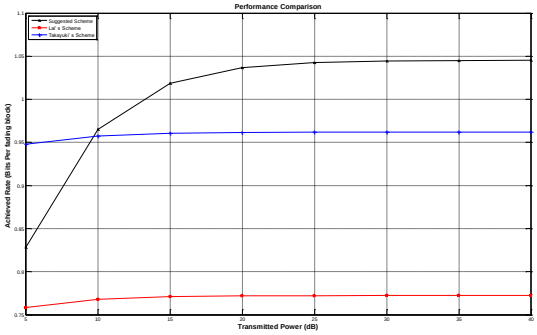

Figure 4: Performance comparison between schemes

That is because as we increase the number of the channel gains composing the randomness source, so the amount of entropy in the constructed source increase.

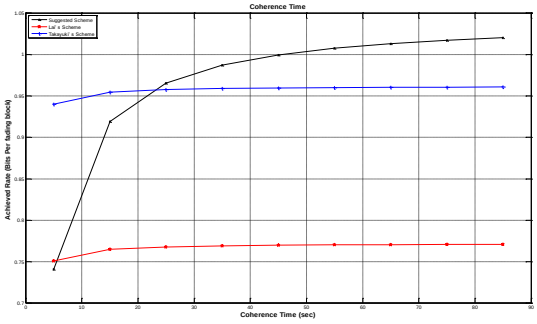

Figure 5: Comparison of the schemes in term of the coherence time

Figure 5 showed the comparison between the three schemes in term of the coherence time. Our protocol had the advantage over the other two schemes when the fading block is more than 23 seconds.

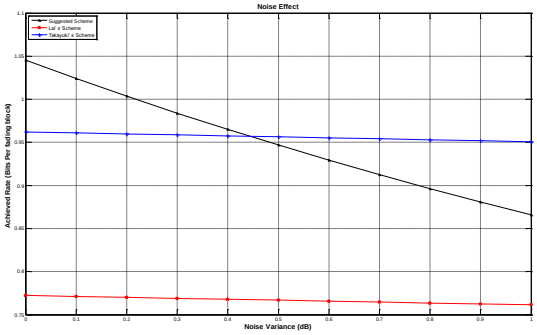

Figure 6: Comparison of the schemes in term of noise effect

Figure 6 showed that the immunity of the schemes that depend on the relaying channel from the effect of noise is better than that depends on a single fading channel. Our scheme had an advantage over other schemes before the noise variance 0.45, after that the scheme rate decrease, that are because there is more terms of noise disturbance in the key rate formulate derived in the previous section.

We can conclude that the randomness source constructed from relaying systems is better than the source constructed from single fading channel in all circumstances such as low transmitted power, short fading period, and high noise at nodes.

6. Conclusions

In this paper, we focused on the generation of secret key based on the wireless channel features. We have suggested a new construction of randomness source based on the FD relaying channel. We considered a situation formed of two legitimate nodes communicated with each other by the aid of a relay to observe the constructed randomness source to establish a shared secret key. The performance of our suggested protocol measured in term of secret key rate, by solving the open problem of estimating the pdf of the product of two physical channel gains. The security analysis of our protocol from a passive eavesdropper and an honest-but-curious relay presented and showed that there is no leakage of information to them due to the independence of the channel coefficients. Because of the numerical simulations, we showed that our randomness source gives more entropy than that of the randomness source based on a single fading channel. The secret key rate of the suggested protocol is better than the secret key rate of protocols based on reciprocity feature of a fading channel.

References

[1] H. Lei, I. Ansari, G. Pan, B. Alomair and M. Alouini, "Secrecy Capacity Analysis Over α - μ Fading Channels", IEEE Communications Letters, vol. 21, no. 6, pp. 1445-1448, 2017.

[2] Sone, Michael, " Physical Layer Security for Wireless Networks Based on Coset Convolutional Coding ", IJCNIS, vol. 12, no. 1, pp. 95-100, 2020.

[3] J. Huang and T. Jiang, "Secret key generation exploiting Ultra-wideband indoor wireless channel characteristics", Security and Communication Networks, vol. 8, no. 13, pp. 2329-2337, 2014.

[4] Y. Shehadeh and D. Hogrefe, "A survey on secret key generation mechanisms on the physical layer in wireless networks", Security and Communication Networks, vol. 8, no. 2, pp. 332-341, 2014.

[5] J. Zhang, T. Duong, A. Marshall and R. Woods, "Key Generation from Wireless Channels: A Review", IEEE Access, vol. 4, pp. 614-626, 2016.

[6] A. Khisti, "Secret-Key Agreement Over Non-Coherent Block-Fading Channels With Public Discussion", IEEE Transactions on Information Theory, vol. 62, no. 12, pp. 7164-7178, 2016.

[7] J. Huang and T. Jiang, "Secret key generation exploiting Ultra-wideband indoor wireless channel characteristics", Security and Communication Networks, vol. 8, no. 13, pp. 2329-2337, 2014.

[8] S. Moosavi, E. Nigussie, S. Virtanen and J. Isoaho, "Cryptographic key generation using ECG signal", 2017 14th IEEE Annual Consumer Communications & Networking Conference (CCNC), 2017.

[9] D. Nguyen, D. Tran, D. Sharma and W. Ma, "On The Study of EEG-based Cryptographic Key Generation", Procedia Computer Science, vol. 112, pp. 936-945, 2017.

[10] C. Zenger, M. Pietersz, J. Zimmer, J. Posielek, T. Lenze and C. Paar, "Authenticated key establishment for low-resource devices exploiting correlated random channels", Computer Networks, vol. 109, pp. 105-123, 2016.

[11] J. N. Laneman, "Cooperative Diversity: Models, Algorithms, and Architectures", Cooperation in Wireless Networks: Principles and Applications, F. H. P. Fitzek and M. D. Katz (Eds.), Chapter 6, Springer, Netherlands, 2006.

[12] X. He and A. Yener, "The Role of Feedback in Two-Way Secure Communications", IEEE Transactions on Information Theory, vol. 59, no. 12, pp. 8115-8130, 2013.
[13] A. Allam, "Improving secret key generation for wireless communications in FDD mode", International Journal of Communication Systems, vol. 31, no. 10, p. e3559, 2018.
[14] T. Shimizu, H. Iwai and H. Sasaoka, "Physical-Layer Secret Key Agreement in Two-Way Wireless Relaying Systems", IEEE Transactions on Information Forensics and Security, vol. 6, no. 3, pp. 650-660, 2011.
[15] H. Zhou, L. Huie and L. Lai, "Secret Key Generation in the Two-Way Relay Channel with Active Attackers", IEEE Transactions on Information Forensics and Security, vol. 9, no. 3, pp. 476-488, 2014.
[16] Goldberg S J, Shah Y C, Reznik A., "Method and apparatus for performing JRNSO in FDD," TDD and MIMO Communications, U.S. Patent Application 12/106, 926[P], 2008.
[17] L. Chen and T. Jiang, "Key Generation Rate in the Full Duplex Relay Wireless Communication Network", Lecture Notes in Electrical Engineering, pp. 285-292, 2017.
[18] L. Lai, Y. Liang and H. Poor, "A Unified Framework for Key Agreement Over Wireless Fading Channels", IEEE Transactions on Information Forensics and Security, vol. 7, no. 2, pp. 480-490, 2012.
[19] A. Khisti, "Secret-Key Agreement Over Non-Coherent Block-Fading Channels With Public Discussion", IEEE Transactions on Information Theory, vol. 62, no. 12, pp. 7164-7178, 2016.
[20] P. Xu, K. Cumanan, Z. Ding, X. Dai and K. Leung, "Group Secret Key Generation in Wireless Networks: Algorithms and Rate Optimization", IEEE Transactions on Information Forensics and Security, vol. 11, no. 8, pp. 1831-1846, 2016.
[21] D. Tse and P. Viswanath, Fundamentals of Wireless Communication. Cambridge, U.K.: Cambridge Univ. Press, 2005.
[22] T. M. Cover and J. A. Thomas, "Elements of Information Theory," New York: Wiley, 1991.
[23] P. Bromiley, "Products and convolutions of Gaussian distributions," Medical School, Univ. Manchester, Manchester, UK, Tech. Rep, vol. 3, p. 2003, 2003.
[24] U. M. Maurer, "Secret key agreement by public discussion from common information", IEEE Transactions on Information Theory, vol. 39, no. 3, pp. 733-742, 1993.
[25] I. Csiszar and P. Narayan, "Common randomness and secret key generation with a helper", IEEE Transactions on Information Theory, vol. 46, no. 2, pp. 344-366, 2000.
[26] M. Médard, "Capacity of correlated jamming channels", in Proc. Allerton Conf. Communication, Control, and Computing, Monticello,IL, Sep. 1997.