GROUP SECRET KEY GENERATION FOR 5G Networks

Ali M. Allam
Department of Electronic, Communication, and Computer Engineering, Helwan University, Cairo, Egypt.
[e-mail: ali_allam@h-eng.helwan.edu.eg]

Received November 9, 2018; revised January 29, 2019; accepted February 22, 2019; published August 31, 2019

Abstract

Key establishment method based on channel reciprocity for time division duplex (TDD) system has earned a vital consideration in the majority of recent research. While most of the cellular systems rely on frequency division duplex (FDD) systems, especially the 5G network, which is not characterized by the channel reciprocity feature. This paper realizes the generation of a group secret key for multi-terminals communicated through a wireless network in FDD mode, by utilizing the nature of the physical layer for the wireless links between them. I consider a new group key generation approach, which using bitwise XOR with a modified pairwise secret key generation approach not based on the channel reciprocity feature. Precisely, this multi-node secret key agreement technique designed for three wireless network topologies: 1) the triangle topology, 2) the multi-terminal star topology, and 3) the multi-node chain topology. Three multi-node secret key agreement protocols suggest for these wireless communication topologies in FDD mode, respectively. I determine the upper bound for the generation rate of the secret key shared among multi-node, for the three multi-terminals topologies, and give numerical cases to expose the achievement of my offered technique.

Keywords: Information-theoretic security, group key generation, channel reciprocity, FDD system, 5G networks

http://doi.org/10.3837/tiis.2019.08.012 **ISSN : 1976-7277**

1. Introduction

Physical layer-based security protocols received a great attention from the researchers in both the security field and the communication filed since Shannon paper [1] and Wyner [2]. From these two papers, the term information theoretical security became in the wireless communication, which divides into two main branches. First, the channel model, which deals with the transmission rate between the communicated nodes to be better than the channel capacity between them and an eavesdropper to maintain the confidentiality of the link without encryption. Second, the source model, which depends on the features of the link between the communicated nodes to share a common randomness source for the generation of a shared secret key.

In many previous pieces of research such as [3]-[5] handled the challenge of establishing a shared secret key as a source model for TDD systems to utilize the benefits of the channel reciprocity in key generation. According to [6], there are five stages to extract a common bit string to be used as a symmetric key from the physical features of a wireless link between a pair of nodes, i.e., single hop connection: channel estimation, randomness extraction, quantization, reconciliation, and privacy application. The purpose of the first two stages is to recognize a common randomness source used for the generation of a secret key, which is under thought in this article. The other stages roles are to extract a number of bits, from the observed randomness source, to be the shared secret key. The noisy observation, between a pair of nodes resulted from the first two stages, needs an extraction procedure to drive reliable bit strings. The secret key rate estimated from the noisy observation regarded as the upper bound rate for the whole process. Moreover, it is common in wireless systems that there is no statistical relationship between opponent channels and legitimate user channels, even if there is a separation by a few centimeters from each other [7]. The establishment of a shared secret between a set of the nodes is more difficult than between two nodes because of the distinctive arbitrary channels related to these nodes.

In [8], they introduced the first group secret key generation based on the source model. After that, a number of tree-based schemes, [9]–[13], adopted the point-to-point mechanism to generate a group secret key among a group of nodes. Moreover, convincing schemes suggested for the generation of a secret key between multi-terminals concerning wireless networks by taking advantage of the channel properties in [14]–[16]. These schemes are more applicable to actual structures at the detriment of some scarification in the rate of the generated secret key in TDD systems. In [17], the authors considered the problem of the group secret key establishment for different models of wireless networks. They merged the approved single-hop key agreement, the segmentation strategy, and the one-time-pad procedure to generate the group key in a TDD system employing the reciprocity feature of the wireless channel.

All the research related to this discipline oriented to the TDD system to get the benefits of the channel reciprocity feature to establish a group shared secret key. Despite that, most of the efficient wireless systems depend on FDD especially 5G networks, there is no, for my knowledge, group key generation scheme suggested for FDD networks. In the FDD system condition, the treatment of two different channels concurrently for transmitting and receiving leads to lose the benefit of the channel reciprocity feature used in the key generation method as in TDD system. Therefore, the characteristics of channel status information (CSI) used in [18]-[20] to create a shared key could not be used directly in FDD mode.

I submit in this paper, a new procedure for generation of a secret key between multi-nodes, without using the reciprocity feature of the linked channels. These nodes are communicated in a different wireless form, especially, the triangle topology, the multi-terminal star topology, and the multi-node chain topology. First, the suggested strategy is validated using a simple triangle wireless topology, where three authorized terminals want to have a common secret key between them without the leakage of any information about that key to anyone outside the group. Moreover, I investigate a more difficult arrangement, star topology, where the secret key generation rate between $N\,(\geq 3)$ authorized terminals are in centralization-shape is derived. Finally, the process of generating the proposed shared secret key for FDD systems offered in the chain topology of wireless networks. My suggested group key establishment approach depends on merging my FDD point-to-point key generation mechanism [21], and the bitwise XOR process. In the following points, I summarize my contribution:

- Figure out the secret key rate for a multi-point wireless communication system in FDD mode.
- **Triangle topology:** I proposed an algorithm for the establishment of a shared secret key between three nodes, based on a bitwise XOR method, for a triangle topology in an FDD mode for 5G networks. The essential part of my suggested algorithm is applying only one-time pad operation between any two FDD-based pairwise key generated among a pair of nodes, and utilize it to generate a shared secret key between the three nodes. Then, the upper bound rate of the generated group key in the suggested algorithm demonstrated.
- **Multi-terminal star network:** an algorithm for the generation of a shared secret key between multi-terminals based on bitwise XOR proposed for a star topology in FDD mode of 5G networks. Where, the central node selects, randomly, a pairwise secret key, and sequential broadcasting the resultant of the bitwise XOR operation between the selected key with all other generated pairwise keys one by one. Then, the upper bound for the generation rate of the group key in the suggested algorithm illustrated.
- **Multi-node chain network:** a bitwise XOR based group key agreement scheme suggested for a chain topology consist of N authorized entities. Then, I derive the upper bound for the group key generated rate.

The choice of the topologies in my suggested schemes came from the relevance of these arrangements for the wireless FDD system.

The remaining of the paper arranged as follows. Section II describes the wireless communication system model under investigation and provides the assumption necessary for my suggested schemes. I revisit the key generation for one hop in FDD mode for 5G networks and determine its secret key rate in sections III for consistency. In section IV, I suggest an algorithm for the group secret key generation for a three-node network. Another scheme for multi-nodes in FDD systems, star topology, is given in section V, and show the impact of the number of terminals on the generated secret key rate. Section VI presents the group key generation for chain networks. Numerical results and comparisons are given in section VII; finally, concluding notes is presented in section VIII.

2. System Model

The system model for the group key generation scheme and its associated system assumption demonstrated as follows.

I'm dealing with the difficulty of establishing a shared secret key among a group of nodes in FDD systems, where N $(N \geq 3)$ authentic nodes desire to produce a shared secret key over a *full-duplex* wireless communication link in the existence of an inactive opponent. In this scheme, all the authentic nodes can send signals over fading links, and they assumed to be full-duplex nodes, i.e., any node uses two different bands for transmission and reception of the signals. Each node n $(n \in \{1, \dots, N\})$ sends a known signal x_n over specific channel use. The signals reached, the other terminals and the eavesdropper are:

$$y_i = h_{n,i} x_n + n_i, \forall i \in \{1, \dots, N\}, i \neq n; \quad (1)$$

$$y_E = h_{n,E} x_n + n_E, \quad (2)$$

where $h_{n,i}$ and $h_{n,E}$ denote the channel status from terminal n to the terminal i, and the eavesdropper, respectively; n_i and n_E are additive white Gaussian noise with zero mean and variance σ^2 at the terminal i and the eavesdropper, respectively.

All the fading coefficients are supposed to be independent and identically distributed, so, $h_{n,i}$ is independent of $h_{n,E}$. Furthermore, I suppose that no node has any information about the channel properties of the communication links before communicating with any node; however, channel state information statistical distributions presented at each terminal. For clarification, I suppose that the channel gains are a univariate normal distribution with zero means. Moreover, in this research, I suppose that all the nodes can transmit and receive simultaneously between each other, i.e., *full-duplex* mode. In addition, I consider that the fading coefficient of the wireless channel remains fixed for a duration *T*. After that, it switches randomly to another independent quantity at the start of every cycle of duration *T*. These recognized as slow block fading model in the literature. Remark that these assumptions regularly utilized in most of the current associated research for the generation of a shared secret key in wireless communication [22]–[24].

For each $n \in \{1, \dots, N\}$, let $S_n = [s_n(1), \dots, s_n(L_n)]^T$ represent the signals sent by terminal n in L_n channel uses. As in [20], **I** suppose that the transmitted power constraint for each terminal is equal for simplicity, i.e.:

$$\frac{1}{L_n} \mathbb{E}\{S_n^T S_n\} \leq P, \forall\, n \in \{1, \dots, N\}. \quad (3)$$

Besides the usage of the wireless channels, those authentic nodes additionally utilize a public channel to exchange messages, which will be overheard by the opponent. This hypothesis of public channel usage has commonly assumed in related works [22]–[24].

The eavesdropper is inactive, which restricts its role in the communication system for receiving only the transmitted information from other members in the system. I express all the exchange messages in the public channel as F. All the authentic nodes in the network desire to have a common secret key among them, by exchanging messages through wireless channels and the public channel. I denote the pairwise key generation function associated with terminal n as f_n, i.e., $K_{N,n} = f_n(S_n, Y_n, F)$, where Y_n is the signals received by terminal n. A group key rate R_{key} is said to be *achievable* if, for any $\epsilon > 0$, there occurs an algorithm and a random variable K_g such that:

$$Pr(K_{N,n} \neq K_g) \leq \epsilon, n = 1, \dots, N, \tag{4}$$

$$\frac{1}{N} I(K_g; F) \leq \epsilon, \tag{5}$$

$$\frac{1}{N} H(K_g) \geq R_{key} - \epsilon. \tag{6}$$

Here (4) expresses that the group key K_g generated at all the nodes depending on the used function is equal with high probability, (5) denotes that the eavesdropper acquires a limited amount of information about the generated group key. Finally, (6) ensure that the rate of the generated key is at least equal to the normalized entropy of the generated key.

3. Pairwise Key Generation For FDD System

In an FDD 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 status, between them. The key generation problem between two nodes, in FDD systems, is more complicated due to the non-reciprocity of the channel gains between the two nodes.

Now, I'm studying the possibility of generating a shared secret key depending on physical layer features of the wireless network in FDD mode with a non-zero rate. This will be the beginning of generating a secret key between a number of users. Followed by another step, which will discuss in the coming sections.

The following algorithm shows the suggested key generation scheme for point-to-point FDD communication mode.

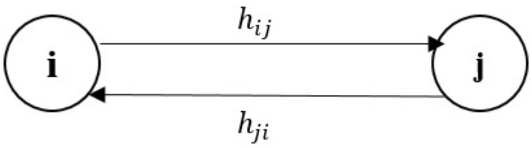


Fig. 1. Single Hop.

The system model for the suggested scheme shown in **Fig. 1**, where two nodes attempt to establish a secret key from the common observation of the composed channel gains of the full duplex link $(h_{ij}h_{ji})$. The corresponding resource element of the scheme shown in **Fig. 2**, where the coherence time T split into two training allocation sequence, forward channel training sequence T_{F_L} and reverse channel training sequence T_{R_L}. I assume that transmission between node i to node j carried over frequency f_1. Simultaneously, from node j to node i carried over frequency f_2.

	← T →	
f_2	1) Node j transmits X.	2) Node j transmits Y_j'.
f_1	1) Node i transmits X.	2) Node i transmits Y_i'.
	← T_{F_L} →	← T_{R_L} →

Fig. 2. Recourse Elements for Point-to-Point Link.

The proposed key generation scheme outlined in Algorithm A.
For channels h_{ij} and h_{ji} , after the forwarding phase of the channel estimation, both nodes receive:

$$Y_j' = h_{ij}X + N_j \tag{7}$$

$$Y_i' = h_{ji}X + N_i \tag{8}$$

Algorithm A: Key Generation Protocol for Point-to-Point Link in FDD mode.

Phase 1: Channel Estimation.

- Node $\boldsymbol{i}$ transmits an identified signal $\boldsymbol{X}$ with transmitted power $\boldsymbol{P}$ over channel $\boldsymbol{h_{ij}}$ to node $\boldsymbol{j}$. Node $\boldsymbol{j}$ receives $\boldsymbol{Y_j'}$. Simultaneously, node $\boldsymbol{j}$ transmits a known signal $\boldsymbol{X}$ with transmitted power $\boldsymbol{P}$ over channel $\boldsymbol{h_{ji}}$ to node $\boldsymbol{i}$. Node $\boldsymbol{i}$ receives $\boldsymbol{Y_i'}$.
- Node $\boldsymbol{i}$ transmits $\boldsymbol{Y_i'}$ with transmitted power $\boldsymbol{P}$ over channel $\boldsymbol{h_{ij}}$ to node $\boldsymbol{j}$. Node $\boldsymbol{j}$ receives $\boldsymbol{Y_j}$ from which it gets the estimation of the common observation $\boldsymbol{\tilde{h}_L^{(j)}}$. Simultaneously, node $\boldsymbol{j}$ transmits $\boldsymbol{Y_j'}$ with power $\boldsymbol{P}$ over channel $\boldsymbol{h_{ji}}$ to node $\boldsymbol{i}$. Node $\boldsymbol{i}$ receives $\boldsymbol{Y_i}$ from which it estimates $\boldsymbol{\tilde{h}_L^{(i)}}$.

Phase 2: Pairwise Key Agreement.

- Both nodes approve the sequence $\boldsymbol{K_L}$ as a shared key, using the correlated estimation pair $\left(\boldsymbol{\tilde{h}_L^{(i)}}, \boldsymbol{\tilde{h}_L^{(j)}}\right)$.

Simultaneously. After that, both of interacted nodes feedback their received signals, after the reverse channel training phase, both nodes receive:

$$Y_i = h_{ji}Y_j' + N_i = h_{ij}h_{ji}X + h_{ji}N_j + N_i \tag{9}$$

$$Y_j = h_{ij}Y_i' + N_j = h_{ij}h_{ji}X + h_{ij}N_i + N_j \tag{10}$$

Simultaneously. From these observations, both nodes get the following estimates:

$$\tilde{h}_L^{(i)} = \frac{X^T}{\|X\|^2} Y_i = h_{ij}h_{ji} + h_{ji}\frac{X^T}{\|X\|^2} N_j + \frac{X^T}{\|X\|^2} N_i \tag{11}$$

$$\tilde{h}_L^{(j)} = \frac{X^T}{\|X\|^2} Y_j = h_{ij}h_{ji} + h_{ij}\frac{X^T}{\|X\|^2} N_i + \frac{X^T}{\|X\|^2} N_j \tag{12}$$

Theorem 1.
The distribution of the common observation $h_{ij}h_{ji}$ is a univariate normal distribution with variance $\frac{\sigma_{ij}^2\sigma_{ji}^2}{\left(\sigma_{ij}^2+\sigma_{ji}^2\right)^2}$ and zero mean.

Proof. For details of the proof, please refer to the appendix section.

So that, $\tilde{h}_L^{(i)}$ is a zero mean Gaussian random variable, with variance $\frac{\sigma_{ij}^2\sigma_{ji}^2}{\left(\sigma_{ij}^2+\sigma_{ji}^2\right)^2}+\frac{\sigma_{ji}^2\frac{\sigma^2}{\|X\|^2}}{\left(\sigma_{ji}^2+\frac{\sigma^2}{\|X\|^2}\right)^2}+\frac{\sigma^2}{\|X\|^2}$, and similarly, $\tilde{h}_L^{(j)}$ is a zero mean Gaussian random variable, with variance,

$$\frac{\sigma_{ij}^2\sigma_{ji}^2}{\left(\sigma_{ij}^2+\sigma_{ji}^2\right)^2}+\frac{\sigma_{ij}^2\frac{\sigma^2}{\|X\|^2}}{\left(\sigma_{ij}^2+\frac{\sigma^2}{\|X\|^2}\right)^2}+\frac{\sigma^2}{\|X\|^2}.$$

From equations (11) and (12), I recognize that there is a common observation $h_{ij}h_{ji}$, from which both nodes can use it as a common randomness source to generate a shared secret key.

Assuming that both nodes transmit signals with transmitted power P during the channel estimation phase, I have $\|X\|^2 = T_{F_L}P$.

Based on the lemma of data processing in [26], it is easy to observe, the validation of the following Markovian relationship [22]:

$$\tilde{h}_L^{(i)} \leftrightarrow Y_i \leftrightarrow h_{ij}h_{ji} \leftrightarrow Y_j \leftrightarrow \tilde{h}_L^{(j)}$$

Which implies $I\left(\tilde{h}_L^{(i)};\tilde{h}_L^{(j)}\right) \leq I(Y_i;Y_j)$.

Similarly, from the Markovian relationship

$$Y_i \leftrightarrow \tilde{h}_L^{(i)} \leftrightarrow h_{ij}h_{ji} \leftrightarrow \tilde{h}_L^{(j)} \leftrightarrow Y_j$$

I have $I\left(\tilde{h}_L^{(i)};\tilde{h}_L^{(j)}\right) \geq I(Y_i;Y_j)$.

As a result of lemma 3.1 in [21], $I\left(\tilde{h}_L^{(i)};\tilde{h}_L^{(j)}\right) = I(Y_i;Y_j)$, which indicates that $\tilde{h}_L^{(i)}$ and $\tilde{h}_L^{(j)}$ maintain the mutual information between Y_i and Y_j; which can be used to compute the rate of a generated secret key between two nodes.

From $\left(\tilde{h}_L^{(i)},\tilde{h}_L^{(j)}\right)$, one can evaluate the secret key rate [27] as following:

$$R_L = \frac{1}{T}\, I\left(\tilde{h}_L^{(i)};\tilde{h}_L^{(j)}\right) \tag{13}$$

$$R_L = \frac{1}{2T}\, log\left(\frac{\left(\frac{\sigma_{ij}^2\sigma_{ji}^2}{\left(\sigma_{ij}^2+\sigma_{ji}^2\right)^2}+\frac{\sigma_{ji}^2\frac{\sigma^2}{\|X\|^2}}{\left(\sigma_{ji}^2+\frac{\sigma^2}{\|X\|^2}\right)^2}+\frac{\sigma^2}{\|X\|^2}\right)\left(\frac{\sigma_{ij}^2\sigma_{ji}^2}{\left(\sigma_{ij}^2+\sigma_{ji}^2\right)^2}+\frac{\sigma_{ij}^2\frac{\sigma^2}{\|X\|^2}}{\left(\sigma_{ij}^2+\frac{\sigma^2}{\|X\|^2}\right)^2}+\frac{\sigma^2}{\|X\|^2}\right)}{\left(\frac{\sigma_{ij}^2\sigma_{ji}^2}{\left(\sigma_{ij}^2+\sigma_{ji}^2\right)^2}+\frac{\sigma_{ji}^2\frac{\sigma^2}{\|X\|^2}}{\left(\sigma_{ji}^2+\frac{\sigma^2}{\|X\|^2}\right)^2}+\frac{\sigma^2}{\|X\|^2}\right)\left(\frac{\sigma_{ij}^2\sigma_{ji}^2}{\left(\sigma_{ij}^2+\sigma_{ji}^2\right)^2}+\frac{\sigma_{ij}^2\frac{\sigma^2}{\|X\|^2}}{\left(\sigma_{ij}^2+\frac{\sigma^2}{\|X\|^2}\right)^2}+\frac{\sigma^2}{\|X\|^2}\right)-\left(\frac{\sigma_{ij}^2\sigma_{ji}^2}{\left(\sigma_{ij}^2+\sigma_{ji}^2\right)^2}\right)^2}\right) \tag{14}$$

Theorem 2.
The key rate of point-to point FDD link is:

$$R_L = \frac{1}{2T} log\left(\frac{\left(\frac{\sigma_{ij}^2\sigma_{ji}^2}{\left(\sigma_{ij}^2+\sigma_{ji}^2\right)^2}+\frac{\sigma_{ji}^2\frac{\sigma^2}{\|X\|^2}}{\left(\sigma_{ji}^2+\frac{\sigma^2}{\|X\|^2}\right)^2}+\frac{\sigma^2}{\|X\|^2}\right)\left(\frac{\sigma_{ij}^2\sigma_{ji}^2}{\left(\sigma_{ij}^2+\sigma_{ji}^2\right)^2}+\frac{\sigma_{ij}^2\frac{\sigma^2}{\|X\|^2}}{\left(\sigma_{ij}^2+\frac{\sigma^2}{\|X\|^2}\right)^2}+\frac{\sigma^2}{\|X\|^2}\right)}{\left(\frac{\sigma_{ij}^2\sigma_{ji}^2}{\left(\sigma_{ij}^2+\sigma_{ji}^2\right)^2}+\frac{\sigma_{ji}^2\frac{\sigma^2}{\|X\|^2}}{\left(\sigma_{ji}^2+\frac{\sigma^2}{\|X\|^2}\right)^2}+\frac{\sigma^2}{\|X\|^2}\right)\left(\frac{\sigma_{ij}^2\sigma_{ji}^2}{\left(\sigma_{ij}^2+\sigma_{ji}^2\right)^2}+\frac{\sigma_{ij}^2\frac{\sigma^2}{\|X\|^2}}{\left(\sigma_{ij}^2+\frac{\sigma^2}{\|X\|^2}\right)^2}+\frac{\sigma^2}{\|X\|^2}\right)-\left(\frac{\sigma_{ij}^2\sigma_{ji}^2}{\left(\sigma_{ij}^2+\sigma_{ji}^2\right)^2}\right)^2}\right) \quad (15)$$

Proof. For details of the proof, please refer to the appendix section**.**

To simplify the equation of the secret key generation rate R_L over a link L , I will assume that the variances of the channel gains for the two paths for a single link are equal, i.e.:

$$\sigma_{ij}^2 = \sigma_{ji}^2 = \sigma_L^2 \quad (16)$$

So,

$$R_L = \frac{1}{2T}\, log\left(\frac{\left(\frac{\sigma_L^2}{2}+\frac{\sigma_L^2\frac{\sigma^2}{PT_{F_L}}}{\left(\sigma_L^2+\frac{\sigma^2}{PT_{F_L}}\right)^2}+\frac{\sigma^2}{PT_{F_L}}\right)^2}{\left(\frac{\sigma_L^2}{2}+\frac{\sigma_L^2\frac{\sigma^2}{PT_{F_L}}}{\left(\sigma_L^2+\frac{\sigma^2}{PT_{F_L}}\right)^2}+\frac{\sigma^2}{PT_{F_L}}\right)^2-\left(\frac{\sigma_L^2}{2}\right)^2}\right) \quad (17)$$

4. Group Key Generation For Triangle Topology

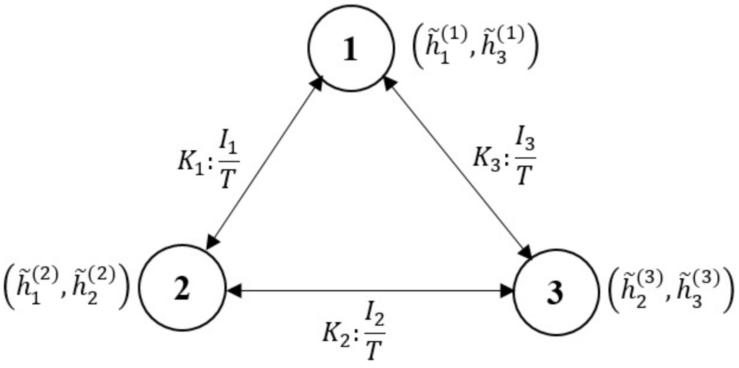

1
$\left(\tilde{h}_1^{(1)}, \tilde{h}_3^{(1)}\right)$
K_1: $\frac{I_1}{T}$
K_3: $\frac{I_3}{T}$
$\left(\tilde{h}_1^{(2)}, \tilde{h}_2^{(2)}\right)$
2
3
$\left(\tilde{h}_2^{(3)}, \tilde{h}_3^{(3)}\right)$
K_2: $\frac{I_2}{T}$

Fig. 3. Triangle Topology.

Now, I'm examining the group key generation problem in its simplest structure between three authentic terminals (i.e., terminals 1, 2 and 3, as presented in **Fig. 3**). For clearness, **I** suppose that all the channel gains of all the paths h_{ij} for the forward transmission and

h_{ji} for the reverse channel, where $i, j \in \{1,2,3\}$, are univariate normal distributions with zero and variance σ_L^2, where $L \in \{1,2,3\}$. A bitwise XOR process based scheme is suggested for this topology to generate a secret key shared between the three terminals, and the associated parameters are recognized. In section V and VI, I will expand my challenge to cover a network consists of more than three nodes.

The proposed bitwise XOR based key generation scheme outlined in Algorithm B, where three authentic terminals begin by point-to-point secret key generation based on the physical layer attributes of the connections between them. Then a group key is created depending on a bitwise XOR mechanism and exchanging messages over the public channel. I present my protocol in Algorithm B.

In the point-to-point key agreement phase, based on the common observation between each pair of terminals (presented in **Fig. 3**) that resultant from the training method and the point-to-point key generation technique in Section III, every two terminals can accept on an approximately uniformly distributed shared secret key K_L with rate $R_L = \frac{I_L}{T}$, where R_L defined as in (17),where $L \in \{1, 2,3\}$.

Algorithm B: Group Key Generation for triangle topology.

Phase 1: Point-to-Point Key Agreement.

- As declared in Section III, point-to-point secret keys can be established depending on the channel fading coefficients of the paths linked with the terminals, where every pair of terminals $(\boldsymbol{i}, \boldsymbol{j})$ permits, over the link between them, a secret key $\boldsymbol{K_L}$, **where** $\boldsymbol{L} \in \{\mathbf{1}, \mathbf{2}, \mathbf{3}\}$.

Phase 2: Group Key Agreement.

- Node 1 broadcasts $\boldsymbol{K_1} \oplus \boldsymbol{K_3}$, so that nodes 1, 2 and 3 can acquire both $\boldsymbol{K_1}$ and $\boldsymbol{K_3}$.
- Nodes 1, 2 and 3 concatenate $(\boldsymbol{K_1} \parallel \boldsymbol{K_3})$ as the resulted secret key for the group.

The phase of group key generation is the most important component of my submitted algorithm. Node 1 sends $K_1 \oplus K_3$ over the public channel, so the other nodes acquire K_1 and K_3. In this case, the three nodes share K_1 and K_3. Clearly, due to the operation of a one-time pad [1], the opponent gains no information about K_1 and K_3. To obtain the group key, I have to concatenate both keys $(K_1 \parallel K_3)$, which achieved with the group key generation rate for triangle topology:

$$R_{Tri} = R_1 + R_3 \tag{18}$$

As revealed, the rate of a group key generation for a triangle topology is equivalent to the summation of the rate of a secret key generation over two links.

5. Group Key Generation In Star Networks

In this section, I examine the generation of a shared secret key between numbers of authentic terminals in a star configuration. A model for the star network, with four authentic terminals, presented in **Fig. 4**. The common observation between the terminals shown in the figure, from which a pairwise secret key K_L generated over each link $L \in$

$\{1,2,\dots,(N-1)\}$ with rate R_L . A bitwise XOR-based scheme suggested for this configuration, and the associated parameters are recognized as follows.

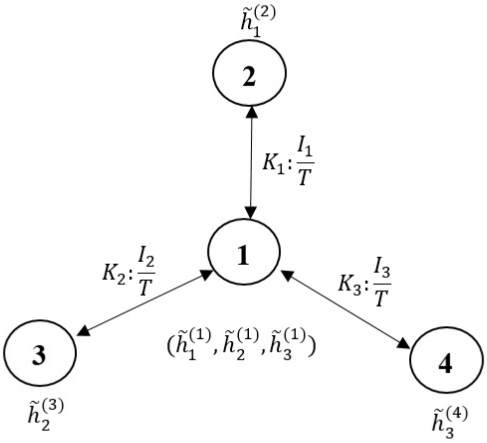


Fig. 4. Star Topology.

As in Section IV, the point-to-point and group key agreements phases summarized in the following key generation protocol, as exposed in Algorithm C.

Algorithm C: Group Key Generation in the Star Topology.

Phase 1: Point-to-Point Key Agreement.

- As stated in Section III, point-to-point secret keys can be generated depending on the channel fading coefficients, where node 1 (the central node) and node $\boldsymbol{i}$, where $\boldsymbol{i} \in \{\boldsymbol{2},\dots,\boldsymbol{N}\}$ agree on a pairwise key $\boldsymbol{K_L}$ for each link, where, $\boldsymbol{L} \in \{\boldsymbol{1},\boldsymbol{2},\dots,(\boldsymbol{N}-\boldsymbol{1})\}$.

Phase 2: Group Key Agreement.

- Node 1 selects randomly $\boldsymbol{K_i}$, where $\in \{\boldsymbol{1},\dots,(\boldsymbol{N}-\boldsymbol{1})\}$, then broadcasts $\boldsymbol{K_i} \oplus \boldsymbol{K_j}$ where $\boldsymbol{j} \in \{\boldsymbol{1},\dots,(\boldsymbol{N}-\boldsymbol{1})\}$ and $\boldsymbol{i} \neq \boldsymbol{j}$,one-by-one, till all the $\boldsymbol{N}$ terminals shared all the keys.
- All the $\boldsymbol{N}$ terminals concatenate these $\boldsymbol{N}-\boldsymbol{1}$ keys $(\boldsymbol{K_1} \parallel \boldsymbol{K_2} \parallel \cdots \parallel \boldsymbol{K_{N-1}})$ as the result group key.

In the point-to-point key agreement phase, based on channel characteristics (presented in **Fig. 4**), and the point-to-point key establishment technique in Section III, N point-to-point secret keys generated by employing the channel characteristics between the terminals, as presented in Section III. Referring to equation (17), the rate of K_L $(L = 1,\dots,N-1)$ derived as $R_L = \frac{I_L}{T}$, where R_L expressed as in equation (17).

In the group key agreement phase, I concatenate the generated $(N-1)$ independent pairwise keys to achieving the concluding shared secret key among the nodes. Initially, the centralized node selects randomly K_i $(i = 1,\dots,N-1)$ and then XORing it with another pairwise key generated in sequence, $K_i \oplus K_j$, and then it delivers results to other nodes over the public channel. Repeat sending these key $(N - 1)$ times till all the N terminals obtain all other keys. Note that the delivering order between these terminals is $(K_1 \oplus K_2, K_1 \oplus K_3, \ldots, K_1 \oplus K_{N-1})$, in case that K_1 is randomly selected by the central node. Clearly, the opponent gains no information about each key, since the one-time pad operation [1] used. Finally, resulting group key $(K_1 \parallel K_2 \parallel K_3 \parallel \cdots \parallel K_{N-1})$ achieved by concatenating these group keys with the rate of:

$$R_{Star} = \sum_{L=1}^{N-1} R_L \tag{19}$$

Assuming the entire generated pairwise secret keys are equal, i.e.:

$$I_1 = I_2 = \cdots = I_{N-1} = I_L \tag{20}$$

$$R_{Star} = \frac{(N-1)}{T} I_L \tag{21}$$

Where, suffix L in the above equation indicates for any link, under the above assumption.

6. Group Key Generation In Chain Network

In this section, Algorithm A suggested for the triangle topology in Section IV is expanded to the chain topology with N authentic nodes. For simplicity, I suppose that all the channel gains of all the paths h_{ij} for the forward transmission and h_{ji} for the reverse channel where $i, j \in \{1, \ldots, N\}$, are univariate normal distributions with zero means and variance σ_L^2, where $L \in \{1, \ldots, N-1\}$.

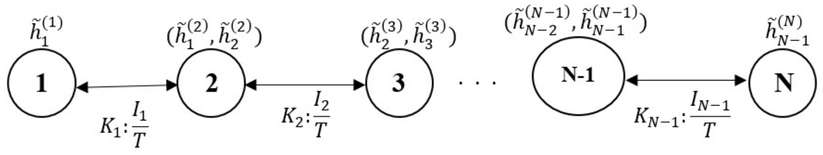

$\tilde{h}_1^{(1)}$
$(\tilde{h}_1^{(2)}, \tilde{h}_2^{(2)})$
$(\tilde{h}_2^{(3)}, \tilde{h}_3^{(3)})$
$(\tilde{h}_{N-2}^{(N-1)}, \tilde{h}_{N-1}^{(N-1)})$
$\tilde{h}_{N-1}^{(N)}$
1
2
3
. . .
N-1
N
K_1: $\frac{I_1}{T}$
K_2: $\frac{I_2}{T}$
K_{N-1}: $\frac{I_{N-1}}{T}$

Fig. 5. Chain Topology.

As presented in Algorithm D, the suggested communication protocol consisted of two phases: point-to-point key agreement and group key agreement.

Algorithm D: Group Key Generation in the Chain Topology.

Phase 1: Point-to-Point Key Agreement.

- As stated in Section III, point-to-point secret keys can be generated depending on the channel fading coefficients, where each adjacent nodes accept a secret key $\boldsymbol{K_L}$, where $\boldsymbol{L} \in \{\mathbf{1}, \ldots, \boldsymbol{N} - \mathbf{1}\}$.

Phase 2: Group Key Agreement.

- Each node from number 2 to $\boldsymbol{N}$, sequentially, broadcasts $\boldsymbol{K_1} \oplus \boldsymbol{K_i}$, where $\boldsymbol{i} \in \{\mathbf{2}, \ldots, \boldsymbol{N} - \mathbf{1}\}$, until all the $\boldsymbol{N}$ nodes acquire $\boldsymbol{K_1}$.
- All the $\boldsymbol{N}$ nodes agree on $\boldsymbol{K_1}$ as the ending group key.

In the point-to-point key agreement phase, based on channel characteristics (presented in **Fig. 5**) and the point-to-point key generation technique in Section III, every adjacent node $(i,j\ ) \in \{(1,2),(2,3),\dots,(N-1,N)\}$, accept a secret key $K_L\ \forall L \in \{1,2,\dots,N-1\}$ from the common observation $(\tilde{h}_L^{(L)},\tilde{h}_L^{(L-1)})$. Therefore, there are $N-1$ separate secret keys. The rate of K_L can express as $R_L\ =\frac{I_L}{T}$, where R_L presented in (17).

In the group key agreement phase: **First**, node 2 forwarding $(K_1 \oplus K_2)$to its neighbor node 3 over a public channel. **Sequentially**, node 2 forwarding $(K_1 \oplus K_3)$ to its neighbor node 4, and so on till the last node. Clearly, the opponent obtains no information about any key, due to the one-time pad operation [1] in the algorithm. The result group key K_1 can be obtained for each node in the chain with the rate,

$$R_{Chain} = R_1 \tag{22}$$

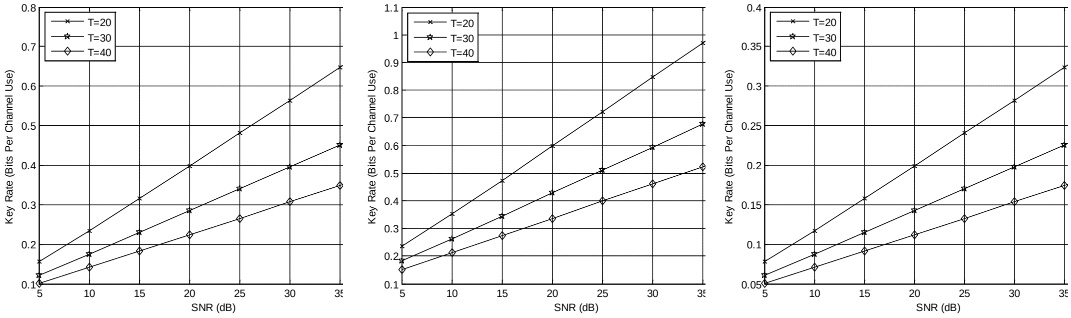
Since a simple bitwise XOR operation is used by the terminals to spread the generated point-to-point keys between terminals in the group key agreement phase, the suggested protocol in both Algorithms C and D has complexity $O(N)$ for a certain time tuple. This means that the suggested schemes have linear complexity corresponding to the number of authentic terminals. Related to the current tree-based schemes in [9]–[11] with polynomial complexity, the suggested schemes in this paper maintain lower complexity.

7. Numerical Results

Now, the analysis concluded in this paper will confirm with some numerical illustrations. I explain the effect of the four parameters (Coherence time – allocation time for training – variance of the channel gain – variance of the noise) on the group secret key generation rate in the three suggested topologies so that I can maintain the positive effect to improve the rate. For simplicity, all noise variances are suggested to be unity (i.e.,$\sigma^2 = 1$). Consequently, the signal-to-noise ratio (SNR) will be reduced to be the transmitted power P.

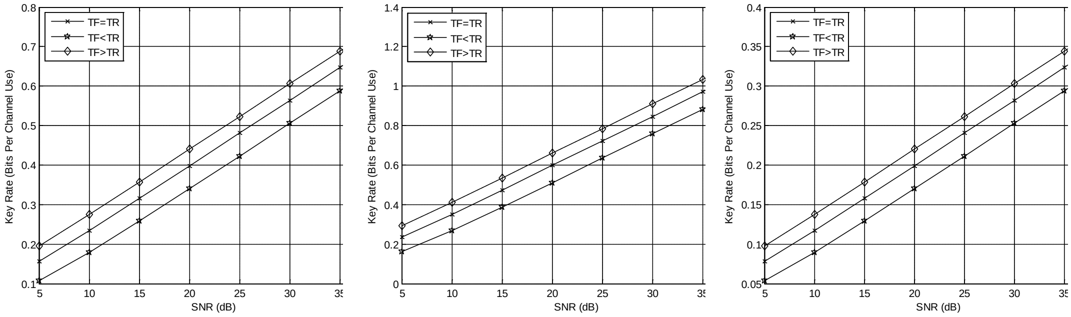
From all the derived equations for the group key rates for the three given topologies, I can conclude that the rate of the star topology is the greater as it increases linearly as the number of nodes increases.

I **first** consider the effect of the channel coherence time, which is one of two variables in the group key rates of the three topologies, on the group secret key rate in the three suggested networks as shown in **Fig. 6**. From this figure, it can observe that the key rate is decreasing as coherence time increase because the normalization factor $1/T$ in the rate is due to the fact that the channel characteristics do not change for the coherence period T, therefore the communication nodes can estimate *only one* value of the channel distribution for every T symbol. Accordingly, my suggested methodology is suitable for slow fading channel situations.



a b c

Fig. 6. Comparison of key rates for different channel coherence time for:
a. Triangle Topology. **b.** Star Topology with N=4. **c.** Chain Topology Network.



a b c

Fig. 7. Comparison of key rates for different Training Duration Distribution for:
a. Triangle Topology. **b.** Star Topology with N=4. **c.** Chain Topology Network.

Secondly, I consider the effect of the duration of the training sequence for both the forward channel and the reverse channel in FDD systems on the secret key rate in the three suggested networks as shown in **Fig. 7**. The figure shows that as the time allocation for forwarding channel-training increase with respect to the part allocated for reverse channel training, the generation rate of the secret key per channel use increase. That is because the individual channel gain estimated during the forwarding path at each node, but the reverse path used only as feedback for the knowledge of the reverse channel gain. This result drives us for improving the rate of my suggested technique, and employ it for future work.

Fig. 8 shows the effect of the channel gain on the group key rate, of course, these gains considered as coefficients in the equation that is why the increase in the curves is constant. I examine the effect of the channel gain variances of reverse and forward paths on the rate with three different values.

I assume the entire channel gains variances are equal and the noise variances are unity. The figure shows that as I increase the channel gain for the paths, the rate increase. This result is because the increase in the channel gain increases the randomness of the common observation between the nodes, which use as the source for the key generation.

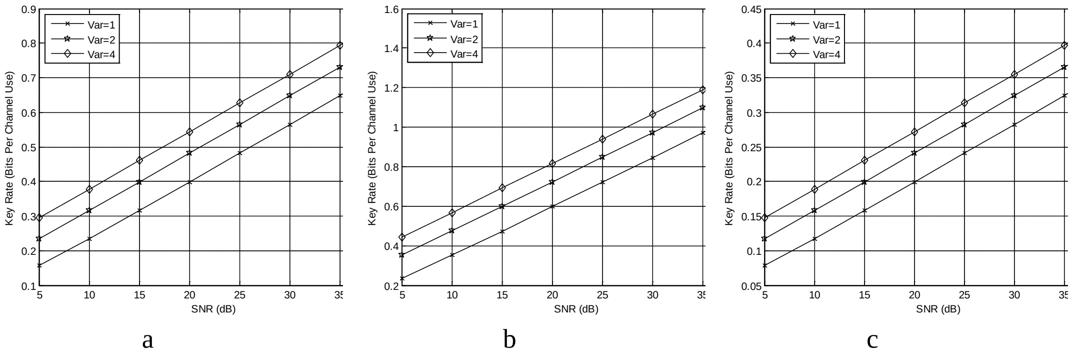


Fig. 8. Comparison of key rates for different channel gain variance for:
a. Triangle Topology. **b.** Star Topology with N=4. **c.** Chain Topology Network.

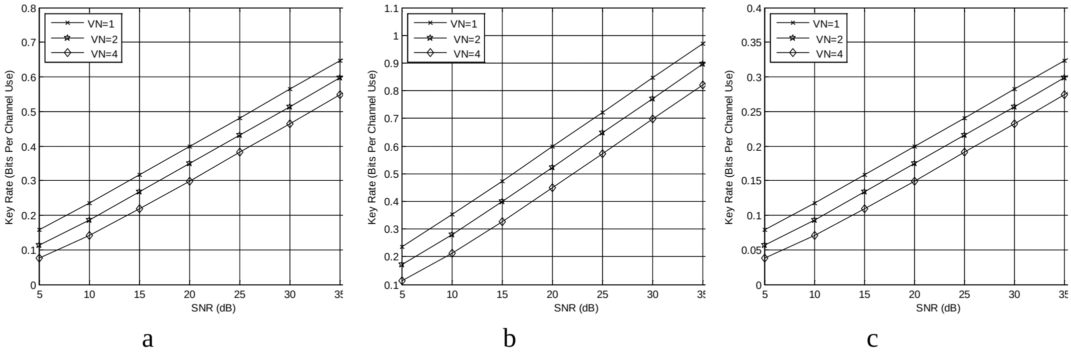


Fig. 9. Comparison of key rates for different noise variance for:
a. Triangle Topology. **b.** Star Topology with N=4. **c.** Chain Topology Network.

In **Fig. 9**, I examine the effect of the noise variances on the group key rate with three different values. I assume the entire channel gains variances are equal to 1. The figure shows that as the noise variance increase, the key rate per channel use decrease. These are due to the effect of the noise on the common observation of the users, which leads to decrease the signal to noise ratio of the common observation. These will reduce the number of common bits, which can be detected to generate the key.

Finally, key rates of star topology examined in **Fig. 10** as a variable of the number of authentic terminals (i.e., N), where T = 15, the variances of all channel characteristics are equal to one, and the power P = 10, 20 or 40. The figure shows the group key rate rates for the star topology increase as the number of authentic nodes increases. That is because they accomplish multiplexing gains $(N\ -1)$, as shown in the equation.

To clarify the performance improvement of my schemes, I compare my proposed schemes with the benchmark schemes in [17] following the same input parameters. **Table 1** summarizes the comparison.

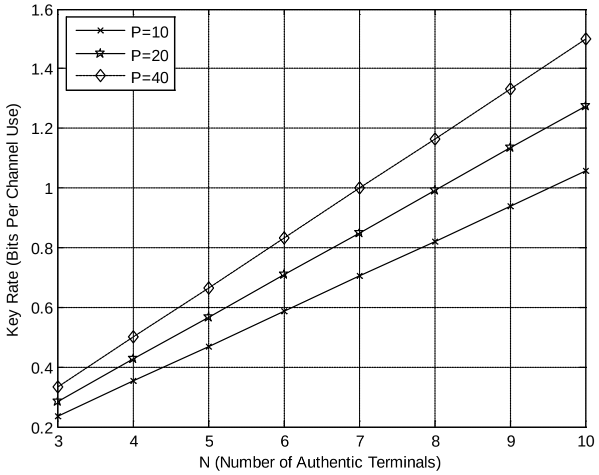


Fig. 10. Comparison of key rates against the number of authentic nodes for different transmitted power in the star topology.

Table 1. Comparison of the performance of the suggested schemes and the benchmark schemes

	Proposed Schemes	Benchmark Work
Used Technology	FDD	TDD
Secret Group Key Rate	Higher for channel gain above 0.25.	Higher for channel gain below 0.25.

In **Table 1**, we held a comparison between our suggested protocol and the benchmark work in [17], which designed for the same purpose and discussed in the introduction section. In [17], the authors suggested a group key generation schemes depending on the reciprocal property of the TDD system, which is not supported for 5G networks. In my suggested schemes, I offered a solution based on FDD technology to support the 5G networks. Besides that, my schemes provided a higher secret group key rate than the benchmark work, and that because the key rate resulting from a single fading channel based randomness source is the smallest and the key rate depending on the FDD system is bigger whatever the value of the transmitted signal. That is because as we increase the number of the channel gains composing the randomness source, the amount of entropy in the constructed source increase.

8. Conclusions

A novel group key generation mechanism with low-complexity, compared with tree-based algorithms, has suggested for various topologies suitable for FDD systems, which depended on the proper merging of my suggested point-to-point key generation approach for FDD systems, and the well-known bitwise XOR operation. My suggested approaches based on the features of fading channel for wireless communication in FDD mode. I applied my suggested approach on triangle topology, star topology and chain topology, which are, the more relevant topologies for wireless communication in FDD mode. From the viewpoint of key generation rate, star topology is the best as the rate increase linearly as the number of nodes increases. In addition, my result shows that the rate of the generated secure key in all suggested topologies can be improved as the reverse training allocation decrease, which can be future work in this trend.

Appendix

Proof of Theorem 1:

Since the two-channel status, h_{ij} and h_{ji} , are assumed to be a univariate normal distribution with variance σ_{ij}^2 and σ_{ji}^2, respectively, and zero mean.

As shown in [25], the product of two Gaussian random variables is a scaled Gaussian distribution, and the scale is Gaussian.

The Product of two Gaussians PDFs $h_{ij} \sim \mathcal{N}\left(\mu_{ij}, \sigma_{ij}^2\right)$ and $h_{ji} \sim \mathcal{N}\left(\mu_{ji}, \sigma_{ji}^2\right)$is:

$$h_{ij} h_{ji} = \frac{S_x}{\sqrt{2\pi\sigma_x^2}} \exp\left[-\frac{(x-\mu_x)^2}{2\sigma_x^2}\right] \tag{23}$$

Where,

$$\sigma_x^2 = \frac{\sigma_{ij}^2\sigma_{ji}^2}{\sigma_{ij}^2+\sigma_{ji}^2} \text{ and } \mu_x = \frac{\mu_{ij}\sigma_{ji}^2+\mu_{ji}\sigma_{ij}^2}{\sigma_{ij}^2+\sigma_{ji}^2} \tag{24}$$

$$S_x = \frac{1}{\sqrt{2\pi\left(\sigma_{ij}^2+\sigma_{ji}^2\right)}} \exp\left[-\frac{\left(\mu_{ij}-\mu_{ji}\right)^2}{2\left(\sigma_{ij}^2+\sigma_{ji}^2\right)}\right] \tag{25}$$

Under my assumption, I have zero mean in all the random variables distribution. Then,

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

For any $X_1 \sim \mathcal{N}(\mu_1, \sigma_1^2)$, $cX_1 = \mathcal{N}(c\mu_1, c^2\sigma_1^2)$, scaling of the normal distribution. So,

$$h_{ij}h_{ji} \sim \mathcal{N}\left(0, \frac{\sigma_{ij}^2\sigma_{ji}^2}{\left(\sigma_{ij}^2+\sigma_{ji}^2\right)^2}\right) \tag{26}$$

Proof of theorem 2:

From [26], I can evaluate the rate of the generated key by:

$$R_L = \frac{1}{T} I\left(\tilde{h}_L^{(i)};\, \tilde{h}_L^{(j)}\right) \tag{27}$$

I can rewrite $R_L$as follows:

$$TR_L = h\left(\tilde{h}_L^{(i)}\right) - h\left(\tilde{h}_L^{(i)} \mid \tilde{h}_L^{(j)}\right) \tag{28}$$

Similar to [28], I have:

$$h\left(\tilde{h}_L^{(i)} \mid \tilde{h}_L^{(j)}\right) = h\left(\tilde{h}_L^{(i)} - a\,\tilde{h}_L^{(j)} \mid \tilde{h}_L^{(j)}\right) \tag{29}$$

$$\leq h\left(\tilde{h}_L^{(i)} - a\,\tilde{h}_L^{(j)}\right) \tag{30}$$

The equality in (30) will hold if I choose a so that $\tilde{h}_L^{(i)} - a\,\tilde{h}_L^{(j)}$and $\tilde{h}_L^{(j)}$are independent and $\left(\tilde{h}_L^{(i)};\, \tilde{h}_L^{(j)}\right)$ are jointly Gaussian. So that,

$$a = Cov\left(\tilde{h}_L^{(i)};\, \tilde{h}_L^{(j)}\right) / \sigma^2_{\tilde{h}_L^{(j)}} \tag{31}$$

Where: $$Cov\left(\tilde{h}_L^{(i)};\, \tilde{h}_L^{(j)}\right) = \mathbb{E}\left\{\tilde{h}_L^{(i)},\, \tilde{h}_L^{(j)}\right\} \tag{32}$$

Since the mean of both $\tilde{h}_L^{(i)}$ and $\tilde{h}_L^{(j)}$ are zero, the covariance:

$$Cov\left(\tilde{h}_L^{(i)};\, \tilde{h}_L^{(j)}\right) = Var\left(h_{ij}h_{ji}\right) = \frac{\sigma_{ij}^2\sigma_{ji}^2}{\left(\sigma_{ij}^2+\sigma_{ji}^2\right)^2} \tag{33}$$

So, the upper bound for $h\left(\tilde{h}_L^{(i)} \mid \tilde{h}_L^{(j)}\right)$ is:

$$h\left(\tilde{h}_L^{(i)} \mid \tilde{h}_L^{(j)}\right) = h\left(\tilde{h}_L^{(i)} - a\,\tilde{h}_L^{(j)}\right) \tag{34}$$

Since $aX_1 = \mathcal{N}(a\mu_1, a^2\sigma_1^2)$.

$$h\left(\tilde{h}_L^{(i)} \mid \tilde{h}_L^{(j)}\right) = \frac{1}{2}log\left(Var\left(\tilde{h}_L^{(i)}\right) - \frac{\left(Var\left(h_{ij}h_{ji}\right)\right)^2}{Var\left(\tilde{h}_L^{(j)}\right)}\right) \tag{35}$$

So:

$$TR_L = \frac{1}{2}log\left(\frac{Var\left(\tilde{h}_L^{(i)}\right)}{Var\left(\tilde{h}_L^{(i)}\right) - \frac{\left(Var\left(h_{ij}h_{ji}\right)\right)^2}{Var\left(\tilde{h}_L^{(j)}\right)}}\right) \tag{36}$$

Accordingly, I can conclude an equation for the secret key generation over a point-to-point link as follows:

$$R_L = \frac{1}{2T}\,log\left(\frac{\left(\frac{\sigma_{ij}^2\sigma_{ji}^2}{\left(\sigma_{ij}^2+\sigma_{ji}^2\right)^2} + \frac{\sigma_{ji}^2\frac{\sigma^2}{\|X\|^2}}{\left(\sigma_{ji}^2+\frac{\sigma^2}{\|X\|^2}\right)^2} + \frac{\sigma^2}{\|X\|^2}\right)\left(\frac{\sigma_{ij}^2\sigma_{ji}^2}{\left(\sigma_{ij}^2+\sigma_{ji}^2\right)^2} + \frac{\sigma_{ij}^2\frac{\sigma^2}{\|X\|^2}}{\left(\sigma_{ij}^2+\frac{\sigma^2}{\|X\|^2}\right)^2} + \frac{\sigma^2}{\|X\|^2}\right)}{\left(\frac{\sigma_{ij}^2\sigma_{ji}^2}{\left(\sigma_{ij}^2+\sigma_{ji}^2\right)^2} + \frac{\sigma_{ji}^2\frac{\sigma^2}{\|X\|^2}}{\left(\sigma_{ji}^2+\frac{\sigma^2}{\|X\|^2}\right)^2} + \frac{\sigma^2}{\|X\|^2}\right)\left(\frac{\sigma_{ij}^2\sigma_{ji}^2}{\left(\sigma_{ij}^2+\sigma_{ji}^2\right)^2} + \frac{\sigma_{ij}^2\frac{\sigma^2}{\|X\|^2}}{\left(\sigma_{ij}^2+\frac{\sigma^2}{\|X\|^2}\right)^2} + \frac{\sigma^2}{\|X\|^2}\right) - \left(\frac{\sigma_{ij}^2\sigma_{ji}^2}{\left(\sigma_{ij}^2+\sigma_{ji}^2\right)^2}\right)^2}\right) \tag{37}$$

References

[1] C. E. Shannon, “Communication theory of secrecy systems,” *Bell Labs Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949. Article (CrossRef Link)

[2] A. D. Wyner, “The wire-tap channel,” *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975. Article (CrossRef Link)

[3] Yuexing Peng, Peng Wang, Wei Xiang, Yonghui Li, "Secret Key Generation Based on Estimated Channel State Information for TDD-OFDM Systems Over Fading Channels," *Wireless Communications IEEE Transactions on*, vol. 16, no. 8, pp. 5176-5186, 2017. Article (CrossRef Link)

[4] S. Zhang, L. Jin, Y. Lou and Z. Zhong, "Secret key generation based on two-way randomness for TDD-SISO system," *China Communications*, vol. 15, no. 7, pp. 202-216, 2018. Article (CrossRef Link)

[5] P. Xu, Z. Ding, X. Dai, and K. K. Leung, "A general framework of wiretap channel with helping interference and state information," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 2, pp. 182–195, Feb. 2014. Article (CrossRef Link)

[6] J. Zhang, T. Q. Duong, A. Marshall, and R. Woods, "Key generation from wireless channels: A review," *IEEE Access*, vol. 4, pp. 614–626, Mar. 2016. Article (CrossRef Link)

[7] V. Granatstein, "Physical principles of wireless communications," *Boca Raton, FL: CRC Press*, 2012.

[8] Csiszár and P. Narayan, "Secrecy capacities for multiple terminals," *IEEE Trans. Inf. Theory*, vol. 50, no. 12, pp. 3047–3061, Dec. 2004. Article (CrossRef Link)

[9] C. Ye and A. Reznik, "Group secret key generation algorithms," in *Proc. of IEEE Int. Symp. Inf. Theory*, pp. 2596–2600, Jun. 2007. Article (CrossRef Link)

[10] S. Nitinawarat, C. Ye, A. Barg, P. Narayan, and A. Reznik, "Secret key generation for a pairwise independent network model," *IEEE Trans. Inf. Theory*, vol. 56, no. 12, pp. 6482–6489, Dec. 2010. Article (CrossRef Link)

[11] S. Nitinawarat and P. Narayan, "Perfect omniscience, perfect secrecy, and Steiner tree packing," *IEEE Trans. Inf. Theory*, vol. 56, no. 12, pp. 6490–6500, Dec. 2010. Article (CrossRef Link)

[12] L. Lai and S.-W. Ho, "Simultaneously generating multiple keys and multi-commodity flow in networks," in *Proc. of IEEE Inf. Theory Workshop (ITW)*, pp. 627–631, Sep. 2012. Article (CrossRef Link)

[13] H. Zhang, L. Lai, Y. Liang, and H. Wang, "The capacity region of the source-type model for secret key and private key generation," *IEEE Trans. Inf. Theory*, vol. 60, no. 10, pp. 6389–6398, Oct. 2014. Article (CrossRef Link)

[14] Q. Wang, H. Su, K. Ren, and K. Kim, "Fast and scalable secret key generation exploiting channel phase randomness in wireless networks," in *Proc. of IEEE INFOCOM*, pp. 1422–1430, Apr. 2011. Article (CrossRef Link)

[15] H. Liu, J. Yang, Y. Wang, and Y. Chen, "Collaborative secret key extraction leveraging received signal strength in mobile wireless networks," in *Proc. of IEEE INFOCOM, Orlando, FL, USA*, pp. 927–935, Mar. 2012.

[16] H. Liu, J. Yang, Y. Wang, Y. Chen, and C. E. Koksal, "Group secret key generation via received signal strength: Protocols, achievable rates, and implementation," *IEEE Trans. Mobile Comput.*, vol. 13, no. 12, pp. 2820–2835, Dec. 2014. Article (CrossRef Link)

[17] P. Xu, K. Cumanan, Z. Ding, X. Dai, and K. Leung, "Group Secret Key Generation in Wireless Networks: Algorithms and Rate Optimization," *IEEE Trans. On Information Forensics and Security*, vol. 11, no. 8, pp. 1831–1846, Aug. 2016. Article (CrossRef Link)

[18] C. Thai, J. Lee, J. Prakash and T. Quek, "Secret Group-Key Generation at Physical Layer for Multi-Antenna Mesh Topology," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 1, pp. 18-33, 2019. Article (CrossRef Link)

[19] T. Tang, T. Jiang and W. Zou, "Group secret key generation in physical layer, protocols and achievable rates," in *Proc. of 2017 17th International Symposium on Communications and Information Technologies (ISCIT)*, 2017. Article (CrossRef Link)

[20] S. Mathur, W. Trappe, N. Mandayam, C. Ye, A. Reznik, "Radio telepathy: Extracting a secret key from an unauthenticated wireless channel," in *Proc. of ACM Conf. Mobile Comput. Network.*, pp. 128-139, Sept. 2008. Article (CrossRef Link)

[21] A. Allam, "A secret key establishment in frequency division duplex communication systems under active attacker," *Security and Privacy*, vol. 1, no. 5, p. e45, 2018. Article (CrossRef Link)

[22] L. Lai, Y. Liang, and H. V. Poor, "A unified framework for key agreement over wireless fading channels," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 480–490, Apr. 2012. Article (CrossRef Link)

[23] G. Li, A. Hu, C. Sun and J. Zhang, "Constructing Reciprocal Channel Coefficients for Secret Key Generation in FDD Systems," *IEEE Communications Letters*, vol. 22, no. 12, pp. 2487-2490, 2018. Article (CrossRef Link)

[24] Y. Peng, P. Wang, W. Xiang and Y. Li, "Secret Key Generation Based on Estimated Channel State Information for TDD-OFDM Systems Over Fading Channels," *IEEE Transactions on Wireless Communications*, vol. 16, no. 8, pp. 5176-5186, 2017. Article (CrossRef Link)

[25] P. Bromiley, "Products and convolutions of Gaussian distributions," *Medical School, Univ. Manchester, Manchester, UK, Tech. Rep*, vol. 3, p. 2003, 2003.

[26] T. M. Cover and J. A. Thomas, "Elements of Information Theory," *2nd ed. Hoboken, New Jersey: John Wiley & Sons, Inc.*, 2006.

[27] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography, Part I: Secret sharing," *IEEE Trans. Inform.Theory*, vol. 39, no. 4, pp. 1121–1132, Jul. 1993. Article (CrossRef Link)

[28] M. Medard, "Capacity of Correlated Jamming Channels," in *Proc. of Allerton Conf. Communication, Control, and Computing,* Monticello, IL, Sep. 1997.

Ali M. Allam received his Ph.D. degree in Communication Engineering from Helwan University in 2008. From 2016 to current works as associated professor in the communication department in Helwan University. His research interests include wireless communication, network security, and cryptography.