Group Secret Key Generation in Wireless Networks: Algorithms and Rate Optimization

Peng Xu, Kanapathippillai Cumanan, *Member, IEEE*, Zhiguo Ding, *Senior, Member, IEEE*, Xuchu Dai and Kin K. Leung *Fellow, IEEE*

***Abstract*—This paper investigates group secret key generation problems for different types of wireless networks, by exploiting physical layer characteristics of wireless channels. A new group key generation strategy with low-complexity is proposed, which combines the well established point-to-point pairwise key generation technique, the multi-segment scheme, and the one-time pad. In particular, this group key generation process is studied for three types of communication networks: 1) the three-node network, 2) the multi-node ring network and 3) the multi-node mesh network. Three group key generation algorithms are developed for these communication networks, respectively. The analysis shows that the first two algorithms yield optimal group key rates, whereas the third algorithm achieves the optimal multiplexing gain. Next, for the first two types of networks, we address the time allocation problem in the channel estimation step to maximize the group key rates. This non-convex max-min time allocation problem is first reformulated into a series of geometric programming, and then a single-condensation-method based iterative algorithm is proposed. Numerical results are also provided to validate the performance of the proposed key generation algorithms and the time allocation algorithm.**

***Index Terms*—Information-theoretic security, group key generation, multiplexing gain, time allocation, geometric programming**

I. Introduction

Recently, secret key generation based on physical layer (PHY) resources and information-theoretic security concepts has received a significant attention. The notion of information-theoretic security was first introduced by Shannon in [1]. In his seminal work, an one-time pad operation was proposed to protect the secret message whose rate cannot exceed the key rate, such that "perfect secrecy" can be achieved. This means that the eavesdropper cannot retrieve any information about the secret message even if it has unlimited computational power. Following this pioneering work, Wyner first utilized a PHY-based approach to realize information-theoretically secure communications in a wiretap channel, where the secrecy capacity was characterized as the difference between the mutual information of the main channel and the eavesdropper channel [2]. This type of models is known as "channel model" in the literature. In recent years, a variety of channel model based approaches have been studied as evidenced by the work in [3]–[5] and the survey in [6], where intelligent channel coding designs are exploited to avoid the requirement of secret keys. However, it has been shown that the secrecy rates achieved by these channel model approaches are limited even with large amount of transmit power, which unintentionally improves the decoding capability of the eavesdropper [4].

In contrast to the channel model based techniques, recently the source model based PHY security approach has received a considerable attention, where correlative source observations between legitimate users are exploited to generate *common randomness* and information-theoretically secure symmetric keys. The works in [7]–[15] aimed to find information-theoretic secrecy key capacities in a variety of source models, however, they have not provided methods to obtain the source observations. Due to channel reciprocity in time-division duplex (TDD) systems, the correlative observations can be obtained via estimates of the wireless fading channels between the legitimate users, which demonstrates the advantages of the source model based key generation approach to support secure multimedia service. Along this direction, many works have investigated this channel reciprocity based key generation problem [16]–[26]. In addition, it is exploited the fact that the eavesdropper channels are independent from channels between the legitimate users as long as the eavesdroppers are half-wavelength away from the legitimate users, which is a general case in wireless networks [27].

The key generation problem between a group of terminals is more challenging due to the different random channels associated with these terminals. The information-theoretic secret key capacity (i.e., the optimal key rate) for the group key generation in the multi-terminal source model was first provided in [10]. Since then, several tree-based algorithms have been developed to achieve the group secret key capacity for the multi-terminal pairwise independent network (PIN) [11]–[15]. On the other hand, effective group key generation algorithms have been proposed for wireless networks by exploiting channel characteristics in [28]–[30]. These algorithms

The work of P. Xu and X. Dai was supported in part by the National Natural Science Foundation of China (NSFC-61471334), in part by the comprehensive strategic cooperation project of the Chinese Academy of Sciences and Guangdong Province (2013B091500065), and in part by China Postdoctoral Science Foundation (2015M570544). The work of Z. Ding and K. Cumanan was supported by H2020-MSCA-RISE-2015 under grant number 690750. The work of Z. Ding was also supported by the Royal Society International Exchange Scheme and the UK EPSRC under grant number EP/N005597/1. Kin K. Leung was financially supported in part by the U.S. Army Research Laboratoryand the U.K. Ministry of Defence and was accomplished under AgreementNumber W911NF-06-3-0001.

P. Xu and X. Dai are with Key Laboratory of Wireless-Optical Communications, Chinese Academy of Sciences, School of Information Science and Technology, University of Science and Technology of China. Address: No. 96 Jinzhai Road, Hefei, Anhui Province, 230026, P. R. China. Kanapathippillai Cumanan is with Department of Electronics, University of York, York, UK, YO10 5DD. Zhiguo Ding is with School of Computing and Communications, Lancaster University, LA1 4WA, UK. Kin K. Leung is with the Department of Electrical and Electronic Engineering, Imperial College, London SW7 2BT, U.K.

are more practical for real systems at the expense of some scarification in the group key rate.

This paper proposes new group key generation algorithms for three types of wireless topologies, namely, the three-node network, the multi-node ring network and the multi-node mesh network. Firstly, this proposed scheme is demonstrated using a simple three-node wireless network, where three legitimate nodes wish to agree on a common group key without revealing this key to an external eavesdropper. Secondly, a more complicated ring network is considered, where the wireless links among the $M(\geq 3)$ legitimate nodes are in ring-shape[1]. Finally, the proposed key generation protocol is extended to the mesh wireless network, where a wireless link exists between every two nodes. To realize optimal or order-optimal group key rates, the propose key generation strategy is based on the careful combination of the well established point-to-point pairwise key generation technique, the multi-segment scheme (i.e., divide each pairwise key into multi-segments [11], [12]), and the one-time pad [1]. The main contributions for each type of wireless network are summarized as follows.

- Three-node network: a two-segment key generation algorithm is proposed for a three-node network, whose main feature is to divide each pairwise key into two segments, and then use them to generate the three-way group key. Then, the optimal rate allocated to each segment is analyzed, and the achievable group key rate of the proposed algorithm is demonstrated to be optimal for the three-node network.
- Multi-node ring network: a multi-segment key generation algorithm is proposed for a ring network with M legitimate nodes, where each pairwise key is divided into $M-1$ segments to a generate group key. Then, the optimal rate allocated to each segment is analyzed, and the group key rate of the proposed algorithm is demonstrated to be optimal for the multi-node ring network.
- Multi-node mesh network: we extend the proposed two-segment based algorithm for the three-node network to a mesh network with M legitimate nodes, where each pairwise key is also divided into two segments for generating group secret keys. This proposed algorithm achieves order-optimal performance among training-based key generation approaches in the mesh wireless network with the optimal multiplexing gain $M/2$ as defined in [21].
- For the first two types of networks, the time allocation is addressed in the training phases to maximize the group key rate. The non-convex time allocation max-min problem is first reformulated into a series of geometric programming through an approximation, and then an iterative algorithm[2] is proposed by exploiting *single condensation method*. In addition, it is proven that the solution obtained through the proposed algorithm satisfies the KKT conditions of the original key rate maximization problem. However, the optimality of the proposed iterative algorithm is validated by comparing with the exhaustive search results.

[1]Formal definitions of a ring network will be given later in this paper. An example of this ring network could arise in a scenario, where a number of legitimate users are located surrounding a mansion, and each of them can only communicate with the nearest two users via wireless channels.

[2]Note that the time allocation algorithms are essentially different from the key generation algorithms, the latter is used to generate keys, while the former is used to maximize the rates of the generated keys.

Now, we briefly explain the difference between the proposed group key generation algorithms and the related existing ones to highlight our contributions. *Firstly*, compared to the key generation problem between two terminals in [19], [21], [22], the group key generation problem considered in this paper is more challenging. Specifically, in the key agreement process, the algorithms in [19], [21], [22] do not give consideration to the multi-segment scheme for each pairwise key, whereas the proposed algorithms not only design the segment-pairing scheme to perform the one-time pad, but also analyze the optimal rate allocated for each segment. *Secondly*, compared to the tree-based algorithms in [11]–[13], the proposed algorithms enjoy high efficiency and low complexity. Specifically, the tree-based group key algorithms divide each pairwise key into multiple one-bit segments. Then, in order to propagate these one-bit segment, the nodes adopt a transmission scheduler via repeatedly finding spanning trees in the corresponding multigraphs. Whereas, the proposed algorithms only divide each pairwise key into a small number of segments with optimal rate allocation, such that only a simple *round robin scheduler* is adopted by the nodes to transmit one-time pads of these segments in the group key agreement. *Finally*, this paper solves the key rate optimization problem with respect to optimal time allocation for some networks, which is nontrivial due to the non-convex characteristic. To the authors' best knowledge, such an optimization problem has not been solved in any existing work.

II. Group Key Generation: Model and Review

In this section, we first define the group key generation system model, and then review some previous related works for the considered model.

A. System Model

We consider a group key generation model, where M ($M \geq 3$) terminals wish to generate a common group secret key through wireless fading channels in the presence of a passive eavesdropper. In this model, all the legitimate terminals can transmit signals over the wireless channels and they are assumed to be *half-duplex* and equipped with a single antenna. Each node m ($m \in \{1, \cdots, M\}$) sends a signal s_m in a given channel use. The received signals at the rest of the nodes and the eavesdropper are

$$\begin{aligned} y_i &= h_{m,i}s_m + n_i,\ \forall i \in \{1, \cdots, M\}, i \neq m; \\ y_E &= h_{m,E}s_m + n_E, \end{aligned} \tag{1}$$

where $h_{m,i}$ and $h_{m,E}$ denote the fading channel coefficients from node m to node i and the eavesdropper, respectively; n_i and n_E are zero mean additive Gaussian noises with variance δ^2 at node i and the eavesdropper, respectively. All the channel gains are assumed to be independent of each other, hence, $h_{m,i}$ is independent of $h_{m,E}$. In addition, it is assumed that none of the terminals have a priori channel state information, however, their distributions are available at each nodes. For simplicity, each channel gain is assumed to be a Gaussian

random variable and the corresponding results can be easily extended to other fading channel coefficients. Moveover, we assume that channels between two nodes are reciprocal, i.e., $h_{i,j} = h_{j,i}$ for $\forall i, j \in \{1, \cdots, M\}$, and they are constant over a period of T symbols and change randomly at the beginning of the next period of T, which is known as a quasi static block fading model in the literature. Note that these assumptions are commonly used in existing related works for key generation in wireless TDD systems [19], [21], [22].

For each $m = 1, \cdots, M$, let $\mathbf{S}_m = [s_m(1), \cdots, s_m(L_m)]^T$ denote the signals transmitted by node m in L_m channel uses. Following [21], we assume that each node transmits signals with an equal power constraint for simplicity, i.e.,

$$\frac{1}{L_m}\mathbb{E}\{\mathbf{S}_m^T\mathbf{S}_m\} \leq P, \forall m \in \{1, \cdots, M\}. \tag{2}$$

In addition to the wireless channels, the legitimate terminals can also use the noiseless public channel with infinite capacity to exchange messages which can be completely accessed by the eavesdropper. This assumption of the public channel access has been widely used in existing literature [7], [8], [22]. The eavesdropper is passive, which means that it only receives from the public and wireless channels and does not send any signals. Let $\mathbf{F}$ denote all the messages transmitted over the public channel. Each of the legitimate terminal exploits the signals received from wireless channels and the public channel to generate a group secret key. Let f_m be the key generation function at node m, i.e., $K_{N,m} = f_m(\mathbf{S}_m, \mathbf{Y}_m, \mathbf{F})$. A group key rate R_{key} is defined to be *achievable*, if for any $\epsilon > 0$, there exists a coding scheme and a random variable K_g such that

$$\begin{aligned} &Pr(K_{N,m} \neq K_g) \leq \epsilon,\ m = 1, \cdots, M, \\ &\frac{1}{N}I(K_g; \mathbf{F}) \leq \epsilon, \\ &\frac{1}{N}H(K_g) \geq R_{key} - \epsilon. \end{aligned} \tag{3}$$

Remark 1: Note that a more general group key generation problem is to share a key among a subgroup of terminals, and the other terminals outside this subgroup act as dedicated helper nodes [10], [12]. Such a general key generation problem has been recognized as a challenging issue, and the key capacity has not been achieved by any existing algorithm. This paper mainly consider the case that all the terminals wish to share the group key. However, the proposed key generation algorithms in the following sections can be extended to this general scenario, based on the combination with cooperative key generation approaches in [21] for the dedicated helper nodes. We will take a mesh network as an example to discuss this issue, as shown later in Section V-C.

B. Review of Previous Works

In this subsection, we review previous related work including the pairwise key and the group key generation schemes.

1) Pairwise key generation: By exploiting the channel reciprocity, the basic idea of the PHY based pairwise key generation (i.e., point-to-point key generation), between each pair of nodes are reviewed here [16], [17], [19], [21], [22]. This will provide necessary background for further development key generation algorithms in this paper. There are two main steps involved the pairwise key generation via wireless fading channel reciprocity: (1) Channel estimation via training symbols and (2) Pairwise key agreement via Slepian-Wolf coding.

In the channel estimation step, each fading block is divided into M phases with each duration T_m, $m = 1, \cdots, M$, where the M nodes take turns to broadcast training sequences in these phases. Suppose node m broadcasts a known sequence $\mathbf{S}_m$ using T_m symbols in each fading block, from which node i obtains the estimate $\tilde{h}_{m,i}$, $\forall i \neq m$. The size of $\mathbf{S}_m$ is $T_m \times 1$ and the corresponding energy is defined as $||\mathbf{S}_m||^2 = T_i P$.

For each channel $h_{i,j}$, $i, j \in 1, \cdots, M$ and $i < j$, the received signals after the training process, at node j and node i can be written as

$$\mathbf{Y}_j^{(i)} = h_{i,j}\mathbf{S}_i + \mathbf{N}_j^{(i)}, \tag{4}$$

$$\mathbf{Y}_i^{(j)} = h_{i,j}\mathbf{S}_j + \mathbf{N}_i^{(j)} \tag{5}$$

in the i-th and the j-th phases, respectively. Then node j and node i can obtain the following estimates:

$$\tilde{h}_{i,j} = \frac{\mathbf{S}_i^T}{||\mathbf{S}_i||^2}\mathbf{Y}_j^{(i)} = h_{j,i} + \frac{\mathbf{S}_i^T}{||\mathbf{S}_i||^2}\mathbf{N}_j^{(i)}, \tag{6}$$

$$\tilde{h}_{j,i} = \frac{\mathbf{S}_j^T}{||\mathbf{S}_j||^2}\mathbf{Y}_i^{(j)} = h_{j,i} + \frac{\mathbf{S}_j^T}{||\mathbf{S}_j||^2}\mathbf{N}_i^{(j)}. \tag{7}$$

In the pairwise key agreement step, each node pair (i, j) can agree on a nearly uniformly distributed pairwise key $K_{i,j} (= K_{j,i})$ with arbitrarily small error probability and the rate is $R_{i,j} = I_{i,j}/T$, where $I_{i,j}$ is defined as [19], [21], [22]

$$\begin{aligned} I_{i,j} &= I_{j,i} = I(\tilde{h}_{i,j}; \tilde{h}_{j,i}) \\ &= -\frac{1}{2}\log\left(1 - \frac{1}{\left(1 + \frac{\delta^2}{\delta_{i,j}^2 PT_i}\right)\left(1 + \frac{\delta^2}{\delta_{i,j}^2 PT_j}\right)}\right). \end{aligned} \tag{8}$$

The above key rate can be achieved based on *Slepian-Wolf coding* and through additional transmissions over the public channel and the additional details can be found in many existing works [19], [21], [22].

2) Group Key Generation: A classical strategy for group key generation using the pairwise keys is to utilize tree-based algorithms related to graphs [11], [12]. The basic idea is to treat the group key generation model as a multigraph, in which each pairwise key rate can be viewed as the weight of the edge associated with the corresponding two nodes. Then, a spanning tree can be found in this multigraph, and the group key information can be propagated over this spanning tree by dividing each pairwise key into multiple one-bit segments and transmitting one-time pads of these segments. By determining the maximal packing of the spanning tree in this multigraph, the achieved group key rate can be obtained, which has been proved to achieve the group key capacity (i.e., the optimal group key rate).

For a given time tuple $(T_1, \cdots, T_M)$, an upper bound on achievable key rates for the training-based group key

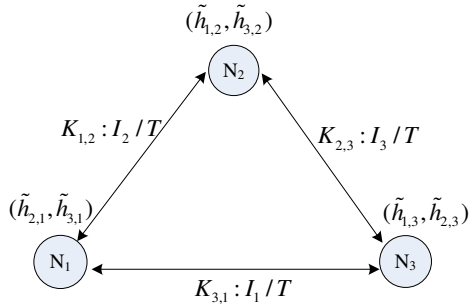


Fig. 1. The wireless network with three legitimate terminals, where each pairwise key and its rate are illustrated. For simplicity, node m is denoted as N_m, $m = 1, 2, 3$.

generation approaches can be expressed as [11], [12]

$$R^M_{upper}(T_1,\cdots,T_M) = \min_{2\le m\le M} \frac{1}{T(m-1)} I'_m(\mathcal{A}), \tag{9}$$

$$\text{where } I'_m(\mathcal{A}) = \min_{(B_1,\cdots,B_m)\in\mathcal{B}_m(\mathcal{A})} \sum_{(i,j):i\in B_l;j\in B_r;l<r} I(\tilde{h}_{i,j},\tilde{h}_{j,i}), \tag{10}$$

when all the M legitimate nodes wish to share a common key. Here $\mathcal{B}_m(A)$ denotes the set of all m-partitions $(B_1,\cdots,B_m)$ with each element B_l, $1 \le l \le m$, intersects with the set $\mathcal{A} = \{1,\cdots,M\}$.

The above upper bound can be achieved by applying existing tree-based algorithms in [11], [12] to the wireless networks. However, in the following sections, we develop simple multi-segment algorithms to achieve or approach the upper bound. In addition, the key rate optimization problem in (9) with respect to time allocation is also solved for some scenarios in Section VI.

III. Group Key Generation Among Three Nodes

In this section, we study the simplest group key generation problem among three legitimate nodes (i.e., nodes 1, 2 and 3, as shown in Fig. 1). For simplicity, we assume that $h_{3,1} \sim \mathcal{N}(0,\delta_1^2)$, $h_{1,2} \sim \mathcal{N}(0,\delta_2^2)$, $h_{2,3} \sim \mathcal{N}(0,\delta_3^2)$. A two-segment based algorithm is proposed for this model and the corresponding parameters are also established. This key generation problem with a larger number of legitimate nodes will be investigated in Section IV and Section V.

A. Key Generation Algorithm

The proposed two-segment based key generation algorithm is summarized in Algorithm A, where the three legitimate nodes first generate pairwise keys based on channel estimation. Then a three-way group key is derived based on a two-segment scheme and through additional communications over the public channel. More details of this algorithm are discussed as follows.

In the pairwise key agreement step, based on channel estimates (shown in Fig. 1) from a training process and the pairwise key generation method in Section II-B, every pair of nodes can agree on a nearly uniformly distributed pairwise key $K_{i,j}$ whose rate is $R_{i,j} = I_1/T$, where I_j is defined as

$$I_j \triangleq I(\tilde{h}_{i,j};\tilde{h}_{j,i}) = \frac{-1}{2}\log\left(1-\frac{1}{\left(1+\frac{\delta^2}{\delta_j^2 PT_i}\right)\left(1+\frac{\delta^2}{\delta_j^2 PT_j}\right)}\right), \tag{11}$$

where $(i,j) \in \{(3,1),(1,2),(2,3)\}$. Since the pairwise key agreement based on channel estimation has been widely studied in many existing works (e.g., [19], [21], [22]), the details are omitted here for simplicity.

The three-way key agreement step is emphasis of the proposed algorithm, in which the two-segment scheme is utilized, i.e., each pairwise key is divided into two independent segments. For example, let $K_{3,1}$ to be $K_{3,1} = (K^3_{3,1}, K^1_{3,1})$, which can be obtained by the one-to-one mapping: $\mathcal{K}_{3,1} \to \mathcal{K}^1_{3,1} \times \mathcal{K}^3_{3,1}$. Such a mapping criteria is known by all the nodes including the eavesdropper. Similar mappings are employed for $K_{1,2}$ and $K_{2,3}$, i.e., $K_{1,2} = (K^1_{1,2}, K^2_{1,2})$ and $K_{2,3} = (K^2_{2,3}, K^3_{2,3})$. Then, node 1 sends $K^1_{3,1} \oplus K^1_{1,2}$ over the public channel, so nodes 2 and 3 can obtain both $K^1_{3,1}$ and $K^1_{1,2}$. In this case, the three nodes choose the one with a smaller rate as the first group key, denoted as $K^1_{3,1} \wedge K^1_{1,2}$. Obviously, the eavesdropper learns nothing about $K^1_{3,1} \wedge K^1_{1,2}$ due to the one-time pad operation. Furthermore, let $R^1_{3,1}$ and $R^1_{1,2}$ denote the rates of $K^1_{3,1}$ and $K^1_{1,2}$, so the rate of $K^1_{3,1} \wedge K^1_{1,2}$ is $\min\{R^1_{3,1}, R^1_{1,2}\}$. Similarly, nodes 2 and 3 send $K^2_{1,2} \oplus K^2_{2,3}$ and $K^3_{2,3} \oplus K^3_{3,1}$, respectively. Hence, the three nodes can obtain the second and the third group keys $K^2_{1,2} \wedge K^2_{2,3}$ and $K^3_{2,3} \wedge K^3_{3,1}$ with rates $\min\{R^2_{1,2}, R^2_{2,3}\}$ and $\min\{R^3_{2,3}, R^3_{3,1}\}$, respectively. Concatenating the three group keys, the final group key $(K^1_{3,1} \wedge K^1_{1,2}, K^2_{1,2} \wedge K^2_{2,3}, K^3_{2,3} \wedge K^3_{3,1})$ can be obtained with the rate

$$R^3_{key} = \min\{R^1_{3,1},R^1_{1,2}\} + \min\{R^2_{1,2},R^2_{2,3}\} + \min\{R^3_{2,3},R^3_{3,1}\}, \tag{12}$$

Algorithm A: Group Key Generation Among Three Nodes

Step 1: Pairwise Key Agreement:

- According to Section II-B, pairwise keys can be generated based on the training process, where the node pair (i,j) agrees on a pairwise key $K_{i,j}$ for $(i,j) \in \{(1,2),(2,3),(3,1)\}$.

Step 2: Three-way Key Agreement:

- Each pairwise key is divided into two independent segments, i.e., $K_{3,1} = (K^3_{3,1}, K^1_{3,1})$, $K_{1,2} = (K^1_{1,2}, K^2_{1,2})$, $K_{2,3} = (K^2_{2,3}, K^3_{2,3})$.
- Node 1 broadcasts $K^1_{1,2} \oplus K^1_{3,1}$, so that nodes 1, 2 and 3 can obtain both $K^1_{1,2}$ and $K^1_{3,1}$. They choose the first group secret key as the one with a smaller rate, denoted as $K^1_{3,1} \wedge K^1_{1,2}$. Similarly, nodes 2 and 3 broadcast $K^2_{2,3} \oplus K^2_{1,2}$ and $K^3_{3,1} \oplus K^3_{2,3}$ respectively, so the three nodes can obtain the second and third group keys, denoted by $K^2_{2,3} \wedge K^2_{1,2}$ and $K^3_{3,1} \wedge K^3_{2,3}$.
- Nodes 1, 2 and 3 concatenate $(K^1_{3,1} \wedge K^1_{1,2}, K^2_{2,3} \wedge K^2_{1,2}, K^3_{3,1} \wedge K^3_{2,3})$ as the final group key.

---

where $R_{i,j}^i + R_{i,j}^j = R_{i,j}$, and $(i,j) \in \{(3,1),(1,2),(2,3)\}$.

B. Optimal Rate Allocation

In this subsection, the optimal rate allocation scheme for each segment is analyzed, i.e., analyzing $(R_{3,1}^1, R_{1,2}^1, R_{1,2}^2, R_{2,3}^2, R_{2,3}^3, R_{3,1}^3)$ in (12), for a fixed time tuple (T_1, T_2, T_3). Then, we establish the group key rate achieved by the proposed algorithm.

Assume that $I_1 \le I_2 \le I_3$, so $R_{3,1} \le R_{1,2} \le R_{2,3}$ and let $R_{3,1}^1 = x_a$, $R_{3,1}^3 = x_b = R_{3,1} - x_a$ for simplicity. Then (12) can be expressed as

$$\begin{aligned} R_{key}^3 = &\min\{x_a, R_{1,2}^1\} + \min\{R_{2,3}^3, x_b\} \\ &+ \min\{R_{1,2} - R_{1,2}^1, R_{2,3} - R_{2,3}^3\}, \end{aligned} \tag{13}$$

where $R_{1,2} \ge R_{1,2}^1$, $R_{2,3} \ge R_{2,3}^3$. We will show that it is optimal to set $R_{1,2}^1 = x_a$ and $R_{2,3}^3 = x_b$. Specifically, R_{key}^3 in (13) can be upper bounded as

$$\begin{aligned} R_{key}^3 &\le \min\{R_{1,2} + \min\{R_{2,3}^3, x_b\}, R_{2,3} + \min\{x_a, R_{1,2}^1\}\} \\ &\le \min\{R_{1,2} + R_{3,1} - x_a, R_{2,3} + x_a\}, \end{aligned} \tag{14}$$

where "$\le$" in each step can be replaced by "=" when $R_{1,2}^1 = x_a$ and $R_{2,3}^3 = x_b = R_{3,1} - x_a$.

Thus, it is optimal to set $x_a^* = [(R_{3,1} + R_{1,2} - R_{2,3})/2]^+ = [(I_1 + I_2 - I_3)/(2T)]^+$, where $[x]^+ = \max\{0, x\}$. Then $R_{key}^3 = \min\{(I_1 + I_2)/T, (I_1 + I_2 + I_3)/(2T)\}$ can be obtained for the case $R_{3,1} \le R_{1,2} \le R_{2,3}$. Symmetrically, by considering other five possible orderings of (I_1, I_2, I_3), the achievable group key rate can be expressed as

$$R_{key}^3 = \frac{1}{T} \min\left\{ I_1 + I_2, I_2 + I_3, I_3 + I_1, \frac{1}{2}(I_1 + I_2 + I_3) \right\}. \tag{15}$$

The following theorem states that the proposed algorithm is optimal in terms of achieved key rates.

Theorem *1:* Among the training-based approaches for secret key generation among three nodes, Algorithm A achieves the optimal key rate for a given tuple (T_1, T_2, T_3), which is defined in (15).

Proof: Setting $M = 3$ in Eq. (9), obviously the upper bound R_{upper}^3 is equal to R_{key}^3 in (15) for a given tuple (T_1, T_2, T_3). Hence Algorithm A achieves the optimal group key rate. ∎

IV. Group Key Generation in Ring Networks

In this section, we study the group key generation problem for a ring network, where M legitimate nodes wish to establish a common key in a ring-shaped topology. To be more specific, assume that $h_{i,j} = h_{j,i} \sim \mathcal{N}(0, \delta_j^2)$ when $(i,j) \in \{(1,2), \cdots, (m, m+1), \cdots, (M-1, M), (M, 1)\}$, and $h_{i,j} = h_{j,i} = \emptyset$ otherwise. Here $\emptyset$ denotes that there does not exist any wireless link between nodes i and j. An example of the ring network with four legitimate nodes is shown in Fig. 2. A multi-segment based algorithm is proposed for this model and the corresponding parameters are also established in the following subsections.

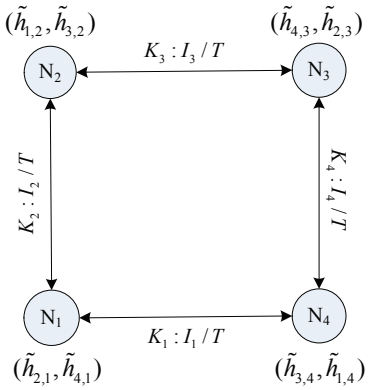


Fig. 2. An example of the ring network with four legitimate nodes, where each pairwise key and its rate are illustrated.

A. Group Key Generation Algorithm

Similar to Section III, the pairwise and group key agreements steps are included in the key generation protocol, as shown in Algorithm B.

In the pairwise key agreement step, based on channel estimates from a training process (shown in Fig. 2) and the pairwise key generation method in Section II-B, M pairwise keys can be generated using the channel estimates, as shown in Section II-B. According to (8), the rate of K_i $(i = 1, \cdots, M)$ can be derived as $R_i = I_i/T$, where I_i can be expressed as

$$\begin{aligned} I_i = I(\tilde{h}_{i,i-1}; \tilde{h}_{i-1,i}) = \\ \frac{-1}{2} \log\left(1 - \frac{1}{\left(1 + \frac{\delta^2}{\delta_i^2 P T_{i-1}}\right)\left(1 + \frac{\delta^2}{\delta_i^2 P T_i}\right)}\right). \end{aligned} \tag{16}$$

In the group key agreement step, we generate M independent group keys to establish the final group key. Firstly, each pairwise key is divided into $M-1$ independent segments, Specifically, let $K_m = (K_m^{]1[}, \cdots, K_m^{]m-1[}, K_m^{]m+1[}, \cdots, K_m^{]M[})$ when $2 \le m \le M-1$, $K_M = (K_M^{]1[}, \cdots, K_M^{]M-1[})$. We denote the rate of the segment $K_j^{]i[}$ as $R_j^{]i[}$ for $\forall i \ne j$.

Secondly, we use these segments of pairwise keys to agree on M group keys. For generation of the m-th group key, $m = 1, \cdots, M$, node m first generates a random key $K^{]m[}$ with a rate [3] $R^{]m[} = \min_{j \in \{1,\cdots,M\}, j \ne m} \{R_j^{]m[}\}$. Specifically, $K^{]m[}$ is generated by randomly and uniformly selecting a element from the set $\{1, \cdots, 2^{R^{]m[}}\}$, which is independent of each pairwise key K_m. Then it delivers $K^{]m[}$ to the next node $m+1$ by sending $K^{]m[} \oplus K_{m+1}^{]m[}$ over the public channel, so that node $m+1$ can decode $K^{]m[}$ since it knows $K_{m+1}^{]m[}$. Repeat delivering this key $M-1$ times until all the M nodes obtain it. Note that the delivering order among these nodes is $(m, m+1, \cdots, M, 0, 1, \cdots, m-1)$. Obviously, the eavesdropper learns nothing about each group $K^{]m[}$, since the one-time pad operation is exploited. Third, the final group key $(K^{]1[}, \cdots, K^{]M[})$ can be obtained by concatenating these

[3] In the key generation process, the rate of each segment is known by all nodes (including the eavesdropper) a priori, so that node m can determine the rate of $K^{]m[}$. Note that a segment is a uniformly distributed random variable, and its rate is a constant, which only represents the value of the entropy but has nothing to do with the randomness of the segment.

Algorithm B: Group Key Generation in the Ring Network

Step 1: Pairwise Key Agreement:

- According to Section II-B, pairwise keys can be generated based on the training process, where nodes M and 1 agree on a pairwise key K_1, and nodes $m-1$ and m agree on a pairwise key K_m, $m=2,\cdots,M$.

Step 2: Group Key Agreement:

- Each pairwise key is divided into $M-1$ independent segments.
- For generation of the m-th group key, node m first generates a random key $K^{]m[}$, then delivers it to the next node (i.e., node $m+1$ when $m<M$, or node 1 when $m=M$), by encrypting it using a certain segment of the pairwise key K_{m+1}. Deliver this group key one-by-one $M-1$ times, until all the M nodes obtain it.
- All the M nodes concatenate these M groups $(K^{]1[},\cdots,K^{]M[})$ as the final group key.

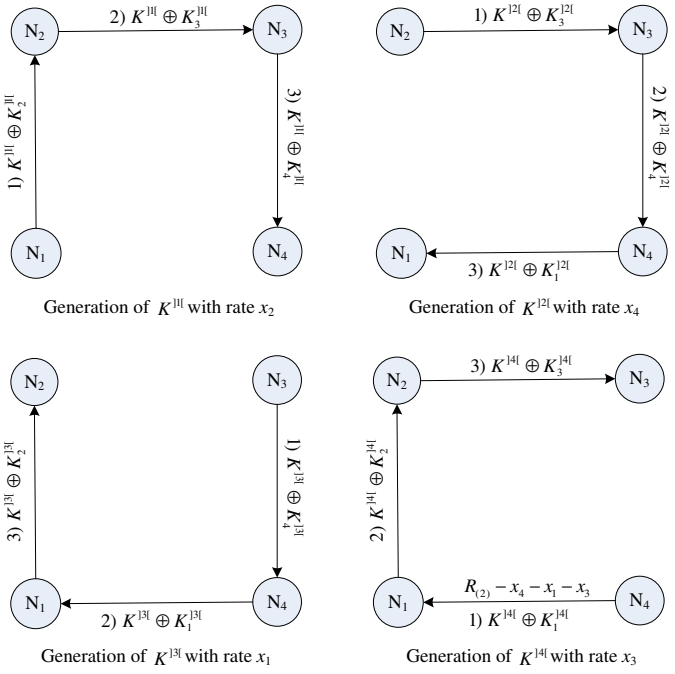


Fig. 3. An example of the group key agreement process with four legitimate nodes, where the ordering of (I_1,I_2,I_3,I_4) is $I_3\le I_1\le I_4\le I_2$, i.e., $(3,1,4,2)=((1),(2),(3),(4))$, and the values of (x_1,x_2,x_3,x_4) are given in Lemma 2.

group keys with the rate of

$$R_{ring}^{M}=\sum_{i=1}^{M}\min_{j\in\{1,\cdots,M\},j\neq i}R_j^{]i[} \tag{17}$$

where $\sum_{i\in\{1,\cdots,M\},i\neq j}R_j^{]i[}=R_j=I_j/T_j$, for $\forall j\in\{1,\cdots,M\}$. An example of the group key agreement process with four legitimate nodes is shown in Fig. 3.

B. Optimal Rate Allocation

In this subsection, the optimal rate allocation scheme for each segment is analyzed, i.e., analyzing the optimal $R_j^{]i[}$ $(i,j\in\{1,\cdots,M\},i\neq j)$ in (17) for a fixed time tuple $(T_1,\cdots,T_M)$. Then, we analyze the group key rate of the proposed algorithm.

Let $R_{(1)}\le R_{(2)}\le\cdots\le R_{(M)}$ be the ordering of the rate tuple $(R_1,R_2,\cdots,R_M)$. Then, (17) can be rewritten as

$$\text{maximize } R_{of}=\sum_{i=1}^{M}\min_{j\in\{1,\cdots,M\},j\neq i}R_{(j)}^{](i)[} \tag{18}$$

$$\text{s.t.}\sum_{i\in\{1,\cdots,M\},i\neq j}R_{(j)}^{](i)[}=R_{(j)},\ \text{for }\forall j\in\{1,\cdots,M\}; \tag{19}$$

$$R_{(j)}^{](i)[}\ge 0,\ \text{for }\forall i\neq j,i,j\in\{1,\cdots,M\}. \tag{20}$$

First, define the min function $\min_{j=2,\cdots,M}R_{(j)}^{](1)[}$ in (18) as x_1. Then according to each equation in (19),

$$x_1=\min_{j=2,\cdots,M}\left\{R_{(j)}-\sum_{i\in\{2,\cdots,M\},i\neq j}R_{(j)}^{](i)[}\right\}. \tag{21}$$

Furthermore, let $x_k\triangleq R_{(1)}^{](k)[}$ for each $k=2,\cdots,M$, so $\sum_{k=2}^{M}x_k=R_{(1)}$. Then we can show that it is optimal to set $R_{(j)}^{](k)[}=x_k$ for $\forall j\neq k$ and $k\neq 1$. Specifically, the objective function R_{of} in (18) can be expressed as

$$R_{of}=x_1+\sum_{i=2}^{M}\min_{j\in\{1,\cdots,M\},j\neq i}R_{(j)}^{](i)[},$$

and its upper bound can be calculated as

$$\begin{aligned}R_{of}&\le x_1+\min_{k=2,\cdots,M}\left\{\sum_{i\in\{2,\cdots,M\},i\neq k}R_{(k)}^{](i)[}\right.\\&\qquad\left.+\min_{j'\in\{1,\cdots,M\},j'\neq k}R_{(j')}^{](k)[}\right\}\\&\le\min_{k=2,\cdots,M}\left\{R_{(k)}+\min_{j'\in\{1,\cdots,M\},j'\neq k}R_{(j')}^{](k)[}\right\}\\&\le\min_{k=2,\cdots,M}\left\{R_{(k)}+x_k\right\},\end{aligned} \tag{22}$$

where "$\le$" in each step can be replaced by "$=$" when $R_{(j)}^{](k)[}=x_k$, $\forall j\neq k$ and $k\neq 1$. This means that it is optimal to set the rate of the segment $K_{(j)}^{](k)[}$ equal to the rate of the segment $K_{(1)}^{](k)[}$, $\forall j\neq k$ and $k\neq 1$. In this case, x_1 can be calculated as

$$\begin{aligned}x_1&=\min_{j=2,\cdots,M}\left(R_{(j)}-\sum_{i\neq 1,i\neq j}x_i\right)\\&=\min_{j=2,\cdots,M}\left(R_{(j)}-R_{(1)}+x_j\right),\end{aligned} \tag{23}$$

where the last relationship is due to the fact that $\sum_{i=2}^{M}x_i=R_{(1)}$. So $x_1\ge 0$ is obtained. Furthermore, since x_2 can be expressed as

$$x_2=R_{(1)}-\sum_{i=3}^{M}x_i, \tag{24}$$

the objective function in (22) and the corresponding optimization problem can be formulated as

$$\text{maximize } R_{of} = \min\left\{R_{(1)} + R_{(2)} - \sum_{i=3}^{M} x_i, R_{(3)} + x_3, \cdots, R_{(M)} + x_M\right\} \quad (25)$$

$$\text{s.t. } x_i \geq 0, i = 2, \cdots, M. \quad (26)$$

The following lemma provides the optimal solution of the above optimization problem, and hence defines the optimal rate allocation policy in (17).

Lemma *2:* For a given rate tuple $(R_{(1)}, \cdots, R_{(M)})$, we have the optimal solution of the optimization problem in (25) with respect to $M-1$ distinct cases.

- Case 1: i.e., $R_{(1)} + R_{(2)} \leq R_{(3)}$, the optimal solution is $x_1^* = R_{(2)}$, $x_2^* = R_{(1)}$, $x_i^* = 0$ for $3 \leq i \leq M$; $R_{of}^* = R_{(1)} + R_{(2)}$.
- Case m ($2 \leq m \leq M-2$): i.e., $\frac{\sum_{j=1}^{m'+1} R_{(j)}}{m'} > R_{(m'+2)}$ for $1 \leq m' \leq m-1$ and $\frac{\sum_{i=1}^{m+1} R_{(j)}}{m} \leq R_{(m+2)}$, the optimal solution is $x_i^* = \frac{\sum_{j=1}^{m+1} R_{(j)}}{m} - R_{(i)}$ for $1 \leq i \leq m+1$, $x_i^* = 0$ for $m+2 \leq i \leq M$; $R_{of}^* = \frac{\sum_{i=1}^{m+1} R_{(j)}}{m}$.
- Case $M-1$: i.e., $\frac{\sum_{j=1}^{m'+1} R_{(j)}}{m'} > R_{(m'+2)}$ for $1 \leq m' \leq M-2$, the optimal solution is $x_i^* = \frac{\sum_{j=1}^{M} R_{(j)}}{M-1} - R_{(i)}$ for $1 \leq i \leq M$; $R_{of}^* = \frac{\sum_{i=1}^{M} R_{(j)}}{M-1}$.

Proof: Refer to Appendix A. ∎

Based on the above lemma, we can conclude that the proposed multi-segment based algorithm is optimal.

Theorem *3:* Among the training-based approaches for secret key generation in the M-node ring network, the proposed multi-segment based algorithm in Algorithm B achieves the optimal key rate for a given tuple $(T_1, \cdots, T_m)$, which can be written as

$$R_{ring}^{M} = \frac{1}{T} \min_{m \in \{2, \cdots, M\}} \frac{\sum_{i=1}^{m} I_{(i)}}{m-1}, \quad (27)$$

where $I_{(1)} \leq \cdots \leq I_{(M)}$ is the ordering of $(I_1, \cdots, I_M)$ with I_i defined in (16).

Proof: An upper bound of the group key rate for the wireless mesh network has been defined in (9). Here, we simplify this upper bound according to the characteristic of the ring network considered in this section. For a given m-partition $(B_1, \cdots, B_m)$ of the set of legitimate nodes $\mathcal{A} = \{1, \cdots, M\}$, denote the number of legitimate nodes in the l-th bin B_l as M_l, where $\sum_{l=1}^{m} M_l = M$, $1 \leq M_l < M$. Then it can be observed that, the term $\sum_{(i,j):i \in B_l; j \in B_r; l<r} I(\tilde{h}_{i,j}, \tilde{h}_{j,i})$ in (10) is formed by the sum of the mutual information with respect to all the wireless links that connect the nodes in different bins. For the ring network, we can show that there exist at least m such wireless links. Specifically, for each $l = 1, \cdots, m$, there are at most $M_l - 1$ wireless links inside bin B_l when $M_l < M$. Hence, at most $\sum_{l=1}^{m}(M_l - 1) = M - m$ links exist inside all the bins. Since the total number of wireless links is M, the smallest number of links that connect the nodes in different bins is $M - (M-m) = m$. In this case, Eq. (10) can be expressed as

$$I'_m(\mathcal{A}) = \min_{\{a_1, \cdots, a_m\} \subseteq \mathcal{A}} \sum_{i=a_1}^{a_m} I_i = \sum_{i=1}^{m} I_{(i)}, \quad (28)$$

where I_i is defined in (16). Then, the upper bound can be simplified as $R_{upper}^{M} = \min_{2 \leq m \leq M} \frac{\sum_{i=1}^{m} I_{(i)}}{T(m-1)}$, which is consistent with (27).

On the other hand, the key rate defined in (27) can be easily obtained via Lemma 2. Hence the proposed multi-segment algorithm achieves the optimal group key rate among training-based approaches. ∎

C. Discussion

This subsection discusses the key rate achieved by applying the two-segment algorithm in Section III to the M-node ring network, where $M \geq 4$.

If we divide each pairwise key into two segments, $2M$ segments can be obtained. Since the generation of a group key requires at least $M-1$ segments obtained from $M-1$ different pairwise keys, at most $\lfloor 2M/(M-1) \rfloor = 2$ group keys can be generated when $M \geq 4$, which require $2(M-1)$ segments and the other two segments are useless. Thus, we only need to divide $M-2$ pairwise keys, and keep the two other pairwise keys undivided. Naturally, we keep the two pairwise keys $K_{(1)}$ and $K_{(2)}$ undivided, and divide each of the other $M-2$ pairwise keys into two segments, i.e., $K_{(m)} \triangleq (K_{(m)}^1, K_{(m)}^2)$, $\forall m \geq 3$.

For the key generation process, two group keys will be generated. Similar to Algorithm B, the first group key K_1 can be generated based on the $M-1$ segments $(K_{(1)}, K_{(3)}^1, \cdots, K_{(M)}^1)$, whose rate is $\min\{R_{(1)}, R_{(3)}^1, \cdots, R_{(M)}^1\}$; the second group key K_2 can be generated based on the $M-1$ segments $(K_{(2)}, K_{(3)}^2, \cdots, K_{(M)}^2)$, whose rate is $\min\{R_{(2)}, R_{(3)}^2, \cdots, R_{(M)}^2\}$. Combing these two group keys, we can obtain the final group key (K_1, K_2) with rate

$$R_{ring}^{two} = \min\{R_{(1)}, R_{(3)}^1, \cdots, R_{(M)}^1\} + \min\{R_{(2)}, R_{(3)}^2, \cdots, R_{(M)}^2\}, \quad (29)$$

where $R_{(m)} = R_{(m)}^1 + R_{(m)}^2$, $\forall m \geq 3$. It is not difficult to prove that the maximum value of R_{ring}^{two} is $\min\{R_{(1)} + R_{(2)}, R_{(3)}, \cdots, R_{(M)}\}$, which can be achieved by setting $R_{(m)}^1 = R_{(1)}$, $\forall m \geq 3$.

In summary, applying the two-segment algorithm in Section III to the M-node ring network, the achievable rate is

$$R_{ring}^{two} = \frac{1}{T} \min\{I_{(1)} + I_{(2)}, I_{(3)}, \cdots, I_{(M)}\}. \quad (30)$$

Remark 2: Comparing (27) and (30), Algorithm B obviously achieves a larger group key rate than the two-segment algorithm, i.e., $R_{ring} \geq R_{ring}^{two}$. This means that dividing each pairwise key into $M-1$ segments is more appropriate than the two-segment scheme, for the M-node ring network.

Algorithm C: Group Key Generation in the Mesh Network

Step 1: Pairwise Key Agreement:

- According to Section II-B, pairwise keys can be generated based on the training process, where every two nodes (i,j), $i<j$, agree on a pairwise key $K_{i,j}(=K_{j,i})$ from the pair of channel estimates $(\tilde{h}_{j,i},\tilde{h}_{i,j})$.

Step 2: Group Key Agreement:

- Each pairwise key is divided into two independent segments, i.e., $K_{i,j}=(K_{i,j}^i,K_{i,j}^j)$, where $K_{i,j}^i$ and $K_{i,j}^j$ can also be expressed as $K_{j,i}^i$ and $K_{j,i}^j$, respectively, $\forall i<j$.
- For generation of the m-th group key, node m first chooses the shortest key among $\{K_{m,l}^m,\forall l\in\{1,\cdots,M\},l\neq m\}$, denoted as K_{m,l_m}^m; then node m broadcasts $K_{m,l_m}^m\oplus K_{m,l}^m$ for $\forall l\neq m\ \&\ l\neq l_m$ over the public channel, such that all the M nodes can obtain this group key K_{m,l_m}^m.
- All the M nodes concatenate $(K_{1,l_1}^1,K_{2,l_2}^2,\cdots,K_{M,l_M}^M)$ as the final group key.

V. Group Key Generation in Mesh Network

In this section, Algorithm A proposed for the three-node scenario in Section III is extended to the wireless mesh network with M legitimate nodes, where every two nodes are connected via a wireless link. Assume that $h_{i,j}=h_{j,i}\sim\mathcal{N}(0,\delta_{i,j}^2)$ for $\forall i,j\in\{1,\cdots,M\}$, $i<j$.

A. Group Key Generation Algorithm

As shown in Algorithm C, the proposed algorithm also includes two key agreement steps: pairwise key agreement and group key agreement.

In the pairwise key agreement step, based on channel estimates from a training process and the pairwise key generation method in Section II-B, every two nodes (i,j), $i<j$, agree on a pairwise key $K_{i,j}(=K_{j,i})$ from the pair of channel estimates $(\tilde{h}_{j,i},\tilde{h}_{i,j})$. Hence, there are $\binom{M}{2}=\frac{M(M-1)}{2}$ independent pairwise keys. The rate of $K_{i,j}$ (=$K_{j,i}$) can be expressed as $R_{i,j}=I_{i,j}/T$ (=$R_{j,i}=I_{j,i}/T$), where $I_{i,j}$ (or $I_{j,i}$) has been given in (8).

In the group key agreement step, each pairwise key is divided into two independent segments, i.e., $K_{i,j}=(K_{i,j}^i,K_{i,j}^j)$ where $K_{i,j}^i$ and $K_{i,j}^j$ can also be expressed as $K_{j,i}^i$ and $K_{j,i}^j$ respectively, $\forall i<j$. The rate of $K_{i,j}^i$ and $K_{i,j}^j$ are defined as $R_{i,j}^i(=R_{j,i}^i)$ and $R_{i,j}^j(=R_{j,i}^j)$, respectively, where $R_{i,j}^i+R_{i,j}^j=R_{i,j}$. Using these segments, all the M legitimate nodes take turns to send messages over the public channel. For each $m=1,\cdots,M$, node m first chooses the shortest key K_{m,l_m}^m among $M-1$ segments, where $l_m=\arg\min_{l\in\{1,\cdots,M\},l\neq m}R_{m,l}^m$. Then, it successively sends $K_{m,l_m}^m\oplus K_{m,l}^m$ for $\forall l\neq m\ \&\ l\neq l_m$, from which node l can obtain K_{m,l_m}^m since it knows $K_{l,m}^m(=K_{m,l}^m)$. Finally, all the M nodes concatenate $(K_{1,l_1}^1,K_{2,l_2}^2,\cdots,K_{M,l_M}^M)$ as the final group key with the rate

$$R_{key}^M=\sum_{m=1}^M R_{m,l_m}^m=\sum_{m=1}^M\min_{l\in\{1,\cdots,M\},l\neq m}R_{m,l}^m,\tag{31}$$

where $R_{m,l}^m+R_{m,l}^l=R_{m,l}(=R_{l,m})=I_{m,l}/T$.

The above key rate generally is not optimal for the wireless mesh networks, however it is order-optimal as shown in the following theorem.

Theorem *4:* Algorithm C achieves the multiplexing gain $M/2$, and such a multiplexing gain is order-optimal.

Proof: On the one hand, set the rates of $K_{m,l}^m$ and $K_{m,l}^l$ to be $R_{m,l}^m=R_{m,l}^l=R_{m,l}/2(=R_{l,m}/2)$. Then according to (31), Algorithm C achieves the following group key rate:

$$\begin{aligned}R_{key}^M&=\frac{1}{2}\sum_{m=1}^M\min_{l\in\{1,\cdots,M\},l\neq m}R_{m,l}\\&=\frac{1}{2T}\sum_{m=1}^M\min_{l\in\{1,\cdots,M\},l\neq m}I_{m,l}.\end{aligned}\tag{32}$$

According to (8), it can be shown that $\lim_{P\to\infty}I_{m,l}/R_s=T$ by setting $T_1=T_2=\cdots=T_M=T/M$, where $R_s=\log P/T$. Based on the definition of the multiplexing gain of a key rate in [21], the multiplexing gain of R_{key}^M is

$$\lim_{P\to\infty}\frac{R_{key}^M}{R_s}=\frac{1}{2T}\sum_{m=1}^M\min_{l\in\{1,\cdots,M\},l\neq m}\left(\lim_{P\to\infty}\frac{I_{m,l}}{R_s}\right)=\frac{M}{2}.\tag{33}$$

On the other hand, by choosing $m=M$ in (9) and (10), the upper bound of the group key rate satisfies:

$$\begin{aligned}R_{upper}^M&\le\frac{1}{T(M-1)}I_M'(\mathcal{A})=\frac{1}{T(M-1)}\times\\&\quad\min_{(B_1,\cdots,B_M)\in\mathcal{B}_M(\mathcal{A})}\sum_{(i,j):i\in B_l;j\in B_r;l<r}I(\tilde{h}_{i,j},\tilde{h}_{j,i})\\&=\frac{1}{T(M-1)}\sum_{i,j\in\{1,\cdots,M\},i<j}I_{i,j},\end{aligned}\tag{34}$$

where the last relationship is due to the fact that there is only one node in each bin B_l for the M-partition of the set of legitimate nodes $\mathcal{A}$. Since there are $\binom{M}{2}=\frac{M(M-1)}{2}$ such $I_{i,j}$, we have

$$\begin{aligned}\lim_{P\to\infty}\frac{R_{upper}^M}{R_s}&\le\frac{1}{T(M-1)}\sum_{i,j\in\{1,\cdots,M\},i<j}\left(\lim_{P\to\infty}\frac{I_{i,j}}{R_s}\right)\\&=\frac{TM(M-1)}{2T(M-1)}=\frac{M}{2}.\end{aligned}\tag{35}$$

Now, it is proved that the achieved multiplexing gain of the proposed algorithm is order-optimal. ■

Remark 3: For the M-node ring network considered in Section IV, the optimal multiplexing gain is $M/(M-1)$, which can be easily derived from Theorem 3. The mesh network achieves a larger multiplexing gain $M/2$ with $M>3$ compared to the ring network. This is due to that each legitimate node in the mesh network can dominate more PHY resources (i.e., wireless channels) for generating a group key.

Remark 4: Since a simple *round robin scheduler* is adopted by the nodes to transmit one-time pads of the segments in the group key agreement, the proposed algorithms (both Algorithms B and C) only have complexity $\mathcal{O}(M)$ for a given time tuple. This means that the proposed algorithms have linear complexity with respect to the number of legitimate nodes. Compared to the existing tree-based algorithms in references [11]–[13] with polynomial complexity, the proposed algorithms enjoy lower complexity.

B. Optimal Rate Allocation

In this subsection, the optimal rate allocation for each segment in (31) is solved for a fixed time tuple $(T_1, \cdots, T_M)$, where the corresponding optimization problem can be formed as follows:

$$\text{maximize } R_{key}^M = \sum_{m=1}^{M} \min_{l\in\{1,\cdots,M\}, l\neq m} R_{m,l}^m, \tag{36}$$

$$\text{s.t. } R_{m,l}^m + R_{m,l}^l = R_{m,l},\ 0 \le R_{m,l}^m \le R_{m,l}, \quad \forall l, m \in \{1,\cdots,M\}, l \neq m. \tag{37}$$

For a fixed time tuple $(T_1, \cdots, T_M)$, this non-convex problem can be transformed into a convex one as follows:

$$\text{maximize } \sum_{m=1}^{M} z_m \tag{38}$$

$$\text{s.t. } z_m \le R_{m,l}^m, \tag{39}$$

$$R_{m,l}^m + R_{m,l}^l = R_{m,l},\ 0 \le R_{m,l}^m \le R_{m,l}, \quad \forall l, m \in \{1,\cdots,M\}, l \neq m. \tag{40}$$

However, a general closed-form solution for the optimal rate allocation of this linear programming problem does not exist, and this optimization problem will be solved later in Section VII using existing convex optimization softwares [31], [32].

C. Discussion

This subsection discusses an achievable multiplexing gain for a general mesh network, based on a simple combination of the proposed algorithm and a cooperative key generation approach in [21]. As defined in [10], [12], only a subgroup of terminals, denoted as $A \triangleq \{1, \cdots, L\}$, wish to share a common key, and the other subgroup of terminals, denoted as $B \triangleq \{L+1, \cdots, M\}$, act as dedicated helper nodes.

We also utilize the training method to generate pairwise keys between every pair of terminals, denoted as $K_{i,j}(= K_{j,i})$ with rate $R_{i,j} = I_{i,j}/T$, where $I_{i,j}$ is defined in (8), $i, j \in \{1, \cdots, M\}$. For the group key generation process, two group keys can be generated. We first utilize the proposed algorithm in Section V-A (i.e., Algorithm C) to generate a group key by exploiting all pairwise keys for the terminal pairs inside group A. Denote this group key as $K_1^{(g)}$. From (32), $K_1^{(g)}$ achieves the rate

$$R_1^{(g)} = \frac{1}{2T} \sum_{m=1}^{L} \min_{l\in A, l\neq m} I_{m,l}. \tag{41}$$

The second group key is generated with the help of the terminals in group B, i.e., it is generated by exploiting all pairwise keys for the terminal pairs (i, j), $\forall i \in A$, $j \in B$. Specifically, based on the cooperative key generation approach in [21], each terminal $j \in B$ sends $K_{j,i_j} \oplus K_{j,i}$, $\forall i \in A,\ i \neq i_j$, over the public channel in turns, where K_{j,i_j} is the shortest key among $\{K_{j,i},\ \forall i \in A\}$. Then, all terminals in A can agree on the key K_{j,i_j} with the rate

$$R_{j,i_j} = \frac{1}{T} \min_{i\in A} I_{j,i},\ \forall j \in B. \tag{42}$$

Concatenating $(K_{j,i_j}, \forall j \in B)$, the second group key can be obtained, denoted as $K_2^{(g)}$. Furthermore, concatenating $(K_1^{(g)}, K_2^{(g)})$, the final group key is generated, whose rate is

$$R_A^{(g)} = R_1^{(g)} + \sum_{j=L+1}^{M} R_{j,i_j}. \tag{43}$$

In the following lemma, $R_A^{(g)}$ is shown to achieve the optimal multiplexing gain in the considered general network.

Lemma *5:* When considering the general group key generation problem among subgroup A, the optimal multiplexing gain can be achieved by simply combining Algorithm C with the cooperative key generation approach in [21], that is $M - L/2$.

Proof: Similar to the proof of Theorem 4, we have $\lim_{P\to\infty} R_1^{(g)}/R_s = L/2$ and $\lim_{P\to\infty} R_{j,i_j}/R_s = 1$, so the achievable multiplexing gain is $L/2 + M - L = M - L/2$.

Furthermore, $M - L/2$ can be proved to be the optimal multiplexing gain. Based on the proof method for Theorem 4 and a general expression of R_{upper}^M in [11] (Lemma 1), it is not difficult to obtain $\lim_{P\to\infty} R_{upper}^M/R_s \le M - L/2$. The details are omitted here for simplicity. ■

VI. Group Key Rate Optimization

In this section, we propose an algorithm to solve key rate optimization problem as shown in (9) with respect to time allocation in the training frame. This optimization problem is non-convex and difficult to be solved in general. In this section, in order to maximize the group key rate, we solve the time allocation problem for two cases: the three-node network and the multi-node ring network. Note that the time allocation problem is solved not only to optimize the proposed multi-segment algorithms but also to optimize the previous tree-based algorithms (e.g., [11], [12]) when applying them in wireless networks. Since a closed-form solution of the linear programming problem in (38)-(40) does not exist for a given time tuple, the optimal time allocation problem for the mesh network in Section V is untractable, which will be solved based on an exhaustive search later in Section VII.

A. Three-Node network

From (9) (or (15)), this problem can be formulated as

$$\text{maximize } \min\left\{I_1+I_2, I_2+I_3, I_3+I_1, \frac{1}{2}(I_1+I_2+I_3)\right\} \tag{44}$$

$$\text{s.t. } \sum_{i=1}^{3} T_i = T,\quad T_i \ge 0,\ i = 1, 2, 3. \tag{45}$$

It can be easily verified that this problem is not convex in terms of $T_i,\ i=1,2,3$ due to the non-convex objective function. Without loss of generality, we rewrite the original problem into the following form:

$$\text{maximize} \quad \tau_0 \tag{46}$$

$$\text{s.t.} \quad I_1+I_2 \geq \tau_0,\ I_2+I_3 \geq \tau_0,\ I_3+I_1 \geq \tau_0,$$
$$\frac{1}{2}(I_1+I_2+I_3) \geq \tau_0, \tag{47}$$

$$\sum_{i=1}^{3} T_i = T,\ T_i \geq 0, i=1,2,3,\ \tau_0 \geq 0. \tag{48}$$

In order to approximate this problem into a convex problem (geometric programming), the equivalent constraints are rewritten as fractions of two posynomials as follows [33]:

$$\text{minimize} \quad \tau_1 \tag{49}$$

$$\text{s.t.} \quad \phi_i(T_1,T_2,T_3) = \frac{f_i(T_1,T_2,T_3)}{g_i(T_1,T_2,T_3)} \leq \tau_1,\ i=1,2,3,$$
$$\phi_4(T_1,T_2,T_3) = \frac{f_4(T_1,T_2,T_3)}{g_4(T_1,T_2,T_3)} \leq \tau_1^2, \tag{50}$$

$$\sum_{i=1}^{3} T_i = T, \quad T_i \geq 0, i=1,2,3,\ \tau_1 \geq 0, \tag{51}$$

$$\text{where} \quad f_1(T_1,T_2,T_3) = \left(\delta^2 {\delta_1}^2 PT_3 + \delta^2 {\delta_1}^2 PT_1 + \delta^4\right) \times \left(\delta^2 {\delta_2}^2 PT_2 + \delta^2 {\delta_2}^2 PT_1 + \delta^4\right) \tag{52}$$

$$g_1(T_1,T_2,T_3) = \left({\delta_1}^2 PT_3 + \delta^2\right)\left(\delta^2 + {\delta_1}^2 PT_1\right) \times \left(\delta^2 + {\delta_2}^2 PT_1\right)\left(\delta^2 + {\delta_2}^2 PT_2\right) = \sum_k g_{1k}(T_1,T_2,T_3), \tag{53}$$

and $f_2(T_1,T_2,T_3)$ (or $g_2(T_1,T_2,T_3)$) and $f_3(T_1,T_2,T_3)$ (or $g_3(T_1,T_2,T_3)$) are similarly defined by substituting $(\delta_1^2,\delta_2^2,T_3,T_1,T_2)$ into $(\delta_2^2,\delta_3^2,T_1,T_2,T_3)$ and $(\delta_3^2,\delta_1^2,T_2,T_3,T_1)$, respectively. Moveover,

$$f_4(T_1,T_2,T_3) = \left({\delta_1}^2 PT_3\delta^2 + \delta^2 {\delta_1}^2 PT_1 + \delta^4\right) \tag{54}$$
$$\times \left(\delta^2 {\delta_2}^2 PT_2 + \delta^2 {\delta_2}^2 PT_1 + \delta^4\right)$$
$$\times \left(\delta^2 {\delta_3}^2 PT_3 + \delta^2 {\delta_3}^2 PT_2 + \delta^4\right) \tag{55}$$

$$g_4(T_1,T_2,T_3) = \left({\delta_1}^2 PT_3 + \delta^2\right)\left(\delta^2 + {\delta_1}^2 PT_1\right) \times \left(\delta^2 + {\delta_2}^2 PT_1\right)\left(\delta^2 + {\delta_2}^2 PT_2\right) \times \left(\delta^2 + {\delta_3}^2 PT_2\right)\left(\delta^2 + {\delta_3}^2 PT_3\right) = \sum_k g_{4k}(T_1,T_2,T_3). \tag{56}$$

Note that here $g_{ik}(T_1,T_2,T_3),\ i=1,2,3,4$ represents the individual summation terms obtained by expanding the corresponding function. The constraints in (50) and (51) are quadratic fractional functions and therefore the corresponding optimization problem cannot be solved directly. However, the original non-convex problem can be converted into a series of geometric programming by exploiting single condensation method. In general, a fractional constraint where both the numerator and the denominator are posynomials, is not convex, whereas the constraint with a posynomial numerator and a monomial denominator is convex [33]. Therefore, the basic idea in single condensation method is to approximate the denominator posynomial into a monomial, which will convert the non-convex constraint into a convex one. Based on this approximation, the posynomials in the denominators of the constraints in (50)-(51) are approximated to the best monomial at a given solution and the optimal time allocations can be efficiently determined. In order to approximate these posynomial into the corresponding monomial the following lemma is required [33]:

Lemma *6:* Let $h(\mathbf{x})$, be a posynomial and defined as

$$h(\mathbf{x}) = \sum_{k=1}^{K} w_k(\mathbf{x}) = \sum_{k=1}^{K} c_k x_1^{n_{1k}} x_2^{n_{2k}} \cdots x_m^{n_{mk}}, \tag{57}$$

where c_k and n_{lk} are the positive constants and arbitrary real numbers, respectively. For this posynomial, the following inequality holds:

$$h(\mathbf{x}) \geq \hat{h}(\mathbf{x}) = \prod_k^K \left(\frac{w_k(\mathbf{x})}{a_k}\right)^{a_k} \tag{58}$$

where $a_k > 0$ and $\sum_{k=1}^{K} a_k = 1$. $\hat{h}(\hat{\mathbf{x}})$ is the best approximation of $h(\hat{\mathbf{x}})$ at a given point $\hat{\mathbf{x}}$ with $a_k = \frac{w_k(\hat{\mathbf{x}})}{h(\hat{\mathbf{x}})}$ and the inequality holds with an equality at this point.

Proof: This can be easily proven based on arithmetic-geometric mean inequality. The proof is omitted here due to space limitation. ■

Based on Lemma 6, the denominator in (50) is rewritten as follows:

$$g_1(T_1,T_2,T_3) = \hat{g}_1(T_1,T_2,T_3) = \prod_k \left(\frac{g_{1k}(T_1,T_2,T_3)}{a_{1k}}\right)^{a_{1k}}, \tag{59}$$

where

$$a_{1k} = \frac{g_{1k}(T_1,T_2,T_3)}{g_1(T_1,T_2,T_3)},\ \forall k \tag{60}$$

Similarly $g_i(T_1,T_2,T_3),\ i=2,3,4$ can be rewritten based on Lemma 6 and the original problem in (49) can be reformulated as

$$\text{minimize} \quad \tau_1 \tag{61}$$

$$\text{s.t.} \quad \tilde{\phi}_i(T_1,T_2,T_3) = \frac{f_i(T_1,T_2,T_3)}{\hat{g}_i(T_1,T_2,T_3)} \leq \tau_1, i=1,2,3,$$
$$\tilde{\phi}_4(T_1,T_2,T_3) = \frac{f_4(T_1,T_2,T_3)}{\hat{g}_4(T_1,T_2,T_3)} \leq \tau_1^2, \tag{62}$$

$$\sum_{i=1}^{3} T_i = T, \quad T_i \geq 0, i=1,2,3,\ \tau_1 \geq 0. \tag{63}$$

The above optimization problem can be formulated into standard geometric programming (convex optimization problem [34]) and can be efficiently solved using existing convex optimization softwares [31], [32]. Based on single condensation method we develop an algorithm, where time allocation is iteratively optimized. The key steps of the proposed algorithm is summarized in Algorithm D.

Next, we show that the solution obtained from Algorithm D satisfies the KKT conditions of the original problem in (44).

This can be proven by validating the following three conditions [35]:

1) $\phi_i(T_1,T_2,T_3) \leq \tilde{\phi}_i(T_1,T_2,T_3),\ \forall\ i,T_1,T_2,T_3.$
2) $\phi_i(T_1^{'},T_2^{'},T_3^{'}) = \tilde{\phi}_i(T_1^{'},T_2^{'},T_3^{'}),\ \forall\ i$, where $T_1^{'},T_2^{'},T_3^{'}$ are the solution obtained from the previous iteration in Algorithm D.
3) $\nabla\phi_i(T_1^{'},T_2^{'},T_3^{'}) = \nabla\tilde{\phi}_i(T_1^{'},T_2^{'},T_3^{'}),\ \forall\ i$

The first condition is satisfied due to $g_i(T_1,T_2,T_3) \geq \hat{g}_i(T_1,T_2,T_3)$, which is developed based on Lemma 6. The second condition can be shown based on the fact that the inequality in (58) is satisfied with equality when $\sum_{k=1}^{K} a_k = 1$ as follows:

$$g_i(T_1,T_2,T_3) = \sum_k g_{ik}(T_1,T_2,T_3),$$

$$\hat{g}_i(T_1,T_2,T_3) = \prod_k \left(\frac{g_{ik}(T_1,T_2,T_3)}{\left(\frac{g_{ik}^{'}(T_1^{'},T_2^{'},T_3^{'})}{g_i(T_1^{'},T_2^{'},T_3^{'})}\right)} \right)^{a_{ik}}, \quad (64)$$

When $(T_1,T_2,T_3) = (T_1^{'},T_2^{'},T_3^{'})$.

$$\hat{g}_i(T_1,T_2,T_3) = \prod_k (g_i(T_1^{'},T_2^{'},T_3^{'}))^{a_{ik}}$$

$$\hat{g}_i(T_1^{'},T_2^{'},T_3^{'}) = \left(g_i(T_1^{'},T_2^{'},T_3^{'})\right)^{\sum_k a_{ik}}. \quad (65)$$

Since $\sum_k a_{ik} = 1$, $\hat{g}_i(T_1^{'},T_2^{'},T_3^{'}) = g_i(T_1^{'},T_2^{'},T_3^{'})$, therefore $\phi_i(T_1^{'},T_2^{'},T_3^{'}) = \tilde{\phi}_i(T_1^{'},T_2^{'},T_3^{'}),\ \forall\ i$. The third condition can be verified by showing $\nabla\hat{g}_i(T_1^{'},T_2^{'},T_3^{'}) = \nabla g_i(T_1^{'},T_2^{'},T_3^{'})$.

$$\hat{g}_i(T_1,T_2,T_3) = \prod_k \left(\frac{g_{ik}(T_1,T_2,T_3)}{\left(\frac{g_{ik}^{'}(T_1^{'},T_2^{'},T_3^{'})}{g_i(T_1^{'},T_2^{'},T_3^{'})}\right)} \right)^{a_{ik}}$$

$$\nabla\hat{g}_i(T_1^{'},T_2^{'},T_3^{'}) = \left[\frac{\partial\hat{g}_i}{\partial T_1}\bigg|_{T_1=T_1^{'}} \frac{\partial\hat{g}_i}{\partial T_2}\bigg|_{T_2=T_2^{'}} \frac{\partial\hat{g}_i}{\partial T_3}\bigg|_{T_3=T_3^{'}} \right]$$

$$\frac{\partial\hat{g}_i}{\partial T_1}\bigg|_{T_1=T_1^{'}} = \left[\prod_k \hat{g}_i(T_1^{'},T_2^{'},T_3^{'})^{a_{ik}} \right] \frac{\sum_j \alpha_j T_1^{-1}}{\hat{g}_i(T_1^{'},T_2^{'},T_3^{'})}$$

$$= \hat{g}_i(T_1^{'},T_2^{'},T_3^{'})^{\sum_k a_{ik}} \times \frac{\sum_j \alpha_j T_1^{-1}}{\hat{g}_i(T_1^{'},T_2^{'},T_3^{'})}$$

$$= \frac{\sum_j \alpha_j}{T_1^{'}} = \frac{\partial g_i}{\partial T_1}\bigg|_{T_1=T_1^{'}}, \quad (66)$$

where α_j's is the a_{ik}'s corresponding to the components of g_{ik}'s with T_1. Similarly, the following derivatives can be verified:

$$\frac{\partial\hat{g}_i}{\partial T_2}\bigg|_{T_2=T_2^{'}} = \frac{\partial g_i}{\partial T_2}\bigg|_{T_2=T_2^{'}}, \quad \frac{\partial\hat{g}_i}{\partial T_3}\bigg|_{T_3=T_3^{'}} = \frac{\partial g_i}{\partial T_3}\bigg|_{T_3=T_3^{'}}. \quad (67)$$

Hence, the solution of Algorithm D satisfies the KKT conditions of the original problem in (44).

Remark 5: In the proposed algorithm, the denominator posynomial is approximated into a monomial in each iteration based on the time allocation obtained from the previous iteration. Therefore, the accuracy of the approximation of the posynomial improves over the number of iterations as the difference between the time allocations obtained from the previous and current iterations decreases. The accuracy of the approximation of the proposed algorithm will be validated through comparison with exhaustive search results in simulations in Section VII.

Algorithm D: Optimal Time Allocation Algorithm Among Three Nodes

Step 1: Initialization of time allocations of T_1, T_2 and T_3
Step 2: Repeat

- Calculate $g_1(T_1,T_2,T_1), g_2(T_1,T_2,T_1), g_3(T_1,T_2,T_1)$ and $g_4(T_1,T_2,T_1)$ for given T_1, T_2 and T_3.
- Calculate $a_{ik},\ i=1,2,3,4,\ \forall k$ from (60)
- Determine $\hat{g}_1(T_1,T_2,T_3),\ \hat{g}_2(T_1,T_2,T_3),\ \hat{g}_3(T_1,T_2,T_3)$ and $\hat{g}_4(T_1,T_2,T_3)$
- Solve the problem in (61)-(63)

Step 3: Until required accuracy.

Remark 6: The computational complexity of the proposed algorithm is less than that of the exhaustive search method. The proposed iterative algorithm solves a geometric programming (convex optimization problem) at each iteration with polynomial time complexity, whereas the exhaustive search method has non-polynomial time complexity. Therefore, the main advantage of the proposed algorithm is the computational complexity reduction.

B. Four-Node Ring Network

In this subsection, we consider the four-node ring network (i.e., $M = 4$) to discuss the optimal time allocation issue. In this case, the optimization problem in (9) (or (27)) can be expressed as

$$\text{maximize } R_{key}^4 = \frac{1}{T}\min\Big\{I_1+I_2, I_1+I_3, I_1+I_4, I_2+I_3, I_2+I_4, I_3+I_4, \frac{1}{2}(I_1+I_2+I_3), \frac{1}{2}(I_1+I_3+I_4), \frac{1}{2}(I_1+I_3+I_4), \frac{1}{2}(I_2+I_3+I_4), \frac{1}{3}(I_1+I_2+I_3+I_4)\Big\}, \quad (68)$$

$$\text{s.t.} \quad \sum_{i=1}^{4} T_i = T, T_i \geq 0, i=1,2,3,4. \quad (69)$$

Without loss of generality, the above max-min problem can be rewritten similar to the problem in (49)-(51) by introducing a new slack variable. In addition, an iterative algorithm can be developed similar to the Algorithm D to find the optimal time allocation based on a series of geometric programming and single condensation method. Due to space limitation, we omit the key steps of the algorithm here. Note that the proposed Algorithm D can be easily extended to a network with different number of nodes.

VII. Numerical Results

In this section, some numerical examples are provided to illustrate the analytical results derived in this paper. For the

TABLE I
THREE-NODE NETWORK WITH THE BLOCK LENGTH $T = 9$

	Equal Time Allocation	Proposed Algorithm	Exhaustive Search
T_1	3	4.31	4.27
T_2	3	4.1	4.14
T_3	3	0.59	0.59
I_1	0.1093	0.0361	0.0360
I_2	1.0632	1.2686	1.2689
I_3	2.0024	1.3107	1.3115
R^3_{key}(BPCU)	0.1303	0.1450	0.1450

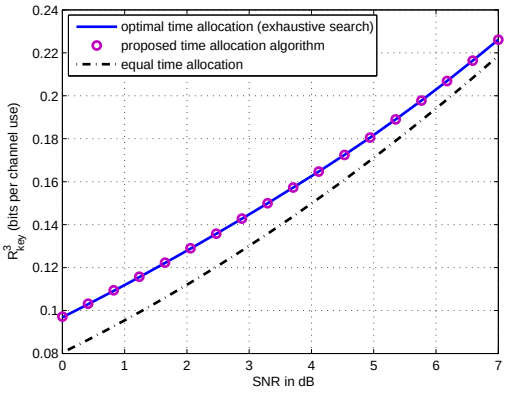


Fig. 4. Illustration of key rate in Eq. (9) or (44) using different time allocation schemes in the three-node network.

TABLE II
FOUR-NODE NETWORK WITH THE BLOCK LENGTH $T = 12$

	Equal Time Allocation	Proposed Algorithm	Exhaustive Search
T_1	3	5.51	5.53
T_2	3	0.23	0.23
T_3	3	0.71	0.71
T_4	3	5.55	5.53
I_1	0.5963	0.9110	0.9110
I_2	2.1029	0.9174	0.9175
I_3	0.0023	5×10^{-5}	5×10^{-5}
I_4	1.4098	0.9133	0.9130
R^4_{ring}(BPCU)	0.0499	0.0759	0.0759

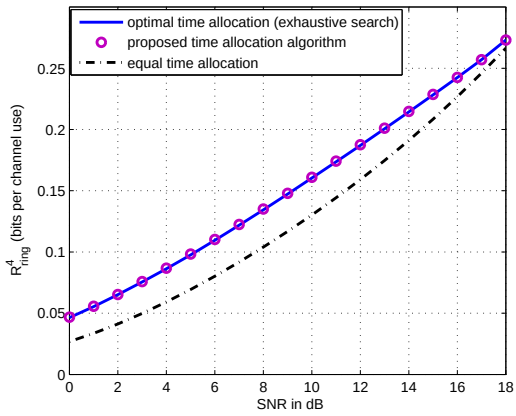


Fig. 5. Illustration of key rate in Eq. (9) or (68) using three time allocation schemes in the four-node ring network.

three-node and ring networks, both the proposed algorithms and existing algorithms in [11], [12] can achieve the optimal key rate, and we mainly illustrate the proposed time allocation algorithms. For the mesh network, the proposed algorithm is compared with the optimal tree-based algorithm [11], [12]. For simplicity, all noise variances are assumed to be one (i.e., $\delta^2 = 1$), therefore the signal-to-noise ratio (SNR) is equal to the power P.

We first consider an asymmetric three-node network, where the variance of each channel gain is $\delta_1^2 = 0.1$, $\delta_2^2 = 1.2$, $\delta_3^2 = 5.1$, and the channel coherence time is $T = 9$. The algorithm is initialized with equal time allocation (i.e., $T_1 = T_2 = T_3 = 3$). Table I represents the simulation results of three time allocation schemes with $P = 2$, where the accuracy of the time distribution is set to 0.01. As can be seen from these results, there is only a slight difference between the results of the proposed algorithm in Section VI-A and the optimal exhaustive search results. Nevertheless, both of them achieve the same group key rate 0.1450 bits per channel use (BPCU), which is bigger than that of the equal time allocation scheme. Fig. 4 depicts more numerical results of these three time allocation schemes. Form this figure, it can be observed that the key rate curve of the proposed iterative algorithm coincides with the one from the exhaustive search scheme, and outperforms the equal time allocation especially at low SNRs. However, differences between these two curves becomes smaller as the SNR increases. This is because the transmit power becomes as the dominant factor in terms of the achievable key rate at high SNRs, and hence the performance improvement using the optimal time allocation is limited. Similar phenomenons are observed in [22] with respective to the optimal power allocation.

Secondly, an asymmetric four-node ring network similar to the previous scenario is also considered, where the variance of each channel gain is assumed to be $\delta_1^2 = 0.5$, $\delta_2^2 = 5.9$, $\delta_3^2 = 0.01$, $\delta_4^2 = 2.1$, and the channel coherence time is set to be $T = 12$. Table II provides the simulation results of three time allocation schemes with $P = 2$, where the required accuracy of the time distribution has been set to the second decimal. As shown in this table, the difference between the results of the proposed algorithm and the optimal exhaustive search scheme is negligible, and both of them achieve the same group key rate 0.0759 BPCU. From Fig. 5, it can be observed that the key rate curve of the proposed iterative algorithm is the same as the one from the exhaustive search scheme. In addition, the proposed iterative algorithm outperforms the equal time allocation.

Thirdly, the key rate of the four-node mesh network is considered as a function of the power P, with $T = 12$, $\delta_{1,3}^2 = \delta_{1,4}^2 = \delta_{2,3}^2 = \delta_{2,4}^2 = \delta_{3,4}^2 = 2.5$, and different values of $\delta_{1,2}^2$. Fig. 6 compares the group key rate of the proposed key generation algorithm (i.e., Eq. (32)) and the optimal upper bound (i.e., Eq. (9)). Note that the optimal rate allocation of Algorithm C in Section V is obtained by solving the linear programming problem in (38), and the optimal time allocation is obtained based on an exhaustive search. As shown in this figure, the proposed algorithm achieves the optimal upper bound only for a symmetric network ($\delta_{1,2}^2 = 2.5$). The reason will be explained. Specifically, Algorithm C achieves the upper

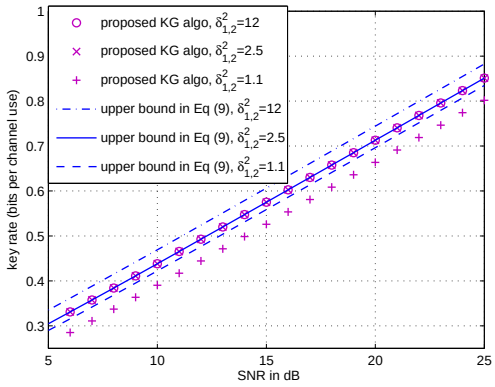


Fig. 6. Key rate of the proposed key generation (KG) algorithm (Eq. (32)) and the optimal upper bound (Eq. (9)) in the four-node mesh network, where $T = 12$, $\delta^2_{1,3} = \delta^2_{1,4} = \delta^2_{2,3} = \delta^2_{2,4} = \delta^2_{3,4} = 2.5$.

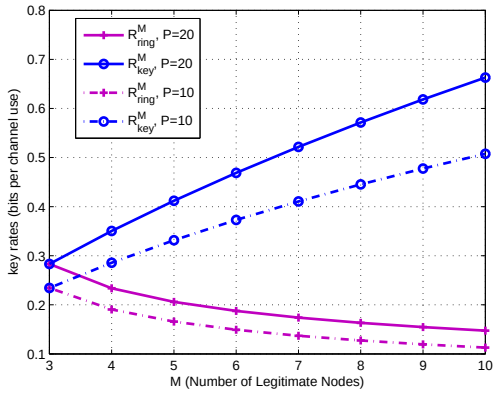


Fig. 7. Key rates of the proposed key generation algorithms for the ring network (Eq. (27)) and mesh network (Eq. (31)) versus the number of legitimate nodes, where $T = 15$, and the variances of all channel gains are unit.

bound in Eq. (34) only when all pairwise keys have the same rate, as discussed in the proof of Theorem 4. Moreover, numerical results demonstrate that an equal time allocation is optimal for the upper bound in Eq. (34) only in a symmetric network, which means that all pairwise keys have the same rate and Algorithm C achieves this upper bound only in the symmetric case. For an asymmetric network ($\delta^2_{1,2} = 1.1$ or 1.2), a gap exists between the key rate curves of the proposed algorithm and the optimal one in Eq. (9). However, this gap remains constant as the SNR increases. This is due to the fact that the proposed algorithm achieves the optimal multiplexing gain as shown in Theorem 4.

Finally, key rates of symmetric ring and mesh networks are considered as a function of the number of legitimate nodes (i.e., M), where $T = 15$, the variances of all channel gains are unit, and the power $P = 10$ or 20. Fig. 7 shows the group key rates of Algorithm B for the ring network and Algorithm C for the mesh network, i.e., R^M_{ring} in Eq. (27) and R^M_{key} in Eq. (31). As shown in this figure, R^M_{ring} decreases with M and R^M_{key} increases with M. This is because they achieve multiplexing gains $M/(M-1)$ and $M/2$, respectively, as discussed in Remark 3.

VIII. Conclusions

A new key generation strategy with low-complexity has been proposed for different types of wireless networks, which is based on the careful combination of well established point-to-point pairwise key generation technique, the multi-segment scheme, and the one-time pad. In the proposed algorithms, each pairwise key is divided into two segments for the three-node network, whereas each pairwise key is divided into $M-1$ segments for the M-node ring network. Both of these algorithms are optimal in terms of the achieved group key rates. Moreover, the proposed two-segment based algorithm for the three-node scenario has been extended to the M-node mesh wireless network and shown to achieve the optimal multiplexing gain $M/2$. Next, the optimal time allocation problems have been solved for some cases where the original non-convex max-min problem is reformulated into a series of geometric programming and an iterative algorithm has been developed by exploiting single condensation method.

Appendix A
Proof of Lemma 2

To obtain the optimal solution of the max-min optimization problem in (25), we consider $(M-2)$ potential steps as follows.

1) Step 1: this step compares $R_{(1)} + R_{(2)}$ and $R_{(3)}$.

If $R_{(1)} + R_{(2)} \le R_{(3)}$, the optimal solution is $x^*_i = 0$ for $3 \le i \le M$. Such a solution maximizes the first term in the min function in (25), and this term becomes $R_{(1)} + R_{(2)}$ now. Furthermore, the objective function achieves the optimal rate $R_{(1)} + R_{(2)}$, since $R_{(1)} + R_{(2)} \le R_{(3)} \le \cdots \le R_{(M)}$ in this case. Moreover, $x^*_2 = R_{(1)}$ can be obtained according to (24), hence $x^*_1 = R_{(2)}$ according to (23).

If $R_{(1)} + R_{(2)} > R_{(3)}$, comparing the first two terms in the min function in (25), obviously it is optimal to set x_3 to be $x_3 = (R_{(1)}+R_{(2)}-R_{(3)}-\sum_{i=4}^{M} x_i)/2$, such that $R_{(1)}+R_{(2)}-\sum_{i=3}^{M} x_i = R_{(3)} + x_3 = (R_{(1)} + R_{(2)} + R_{(3)} - \sum_{i=4}^{M} x_i)/2$. Then, one can refer to the following steps to find the optimal tuple $(x^*_1, \cdots, x^*_M)$.

The derivations from step 2 to $(M-2)$ can be summarized as follows:

2) Step m($2 \le m \le M-2$): this step corresponds to the case

$$\frac{\sum_{j=1}^{m'+1} R_{(j)}}{m'} > R_{(m'+2)} \text{ for } 1 \le m' \le m-1. \tag{70}$$

Moreover, the optimization problem in this step is formulated as

$$\text{maximize } R_{of} = \min \left\{ \frac{\sum_{j=1}^{m+1} R_{(j)} - \sum_{i=m+2}^{M} x_i}{m}, \right. \\ \left. R_{(m+2)} + x_{m+2}, \cdots, R_{(M)} + x_M \right\} \tag{71}$$

$$\text{s.t. } x_i \ge 0, i = 2, \cdots, M, \tag{72}$$

where x_2 is given in (24) and x_i is iteratively given by

$$x_i = \frac{\sum_{j=1}^{i-1} R_{(j)} - (i-2)R_{(i)} - \sum_{i'=i+1}^{M} x_{i'}}{i-1} \quad \text{for } 3 \le i \le m+1. \tag{73}$$

These $m-1$ relationships are iteratively obtained from step 1 to step $m-1$.

Now, we will compare $\frac{\sum_{i=1}^{m+1} R_{(j)}}{m}$ and $R_{(m+2)}$. First consider the case that

$$\frac{\sum_{j=1}^{m+1} R_{(j)}}{m} \le R_{(m+2)}. \tag{74}$$

Obviously the optimal solution is $x_i^* = 0$ for $m+2 \le i \le M$. Then, when $3 \le i \le m+1$, x_i can be obtained using the iterative relationship in (73) and the inductive method:

- Since $x_i = 0$ for $m+2 \le i \le M$, according to (73),

$$\begin{aligned} x_{m+1} &= \frac{\sum_{j=1}^{m} R_{(j)} - (m-1)R_{(m+1)}}{m} \\ &= \frac{\sum_{j=1}^{m+1} R_{(j)}}{m} - R_{(m+1)}. \end{aligned} \tag{75}$$

  Note that when $m = 2$, x_3 is given by the above equation and this problem has been solved. When $m \ge 3$, we carry out with the following inductive process.

- Assume that $x_{i'} = \frac{\sum_{j=1}^{m+1} R_{(j)}}{m} - R_{(i')}$ for $i+1 \le i' \le m+1$, where $3 \le i \le m$, then $\sum_{i'=i+1}^{M} x_{i'}$ can be calculated as

$$\begin{aligned} \sum_{i'=i+1}^{M} x_{i'} &= \sum_{i'=i+1}^{m+1} x_{i'} = \sum_{i'=i+1}^{m+1} \left(\frac{\sum_{j=1}^{m+1} R_{(j)}}{m} - R_{(i')} \right) \\ &= \frac{m-i+1}{m} \sum_{j=1}^{m+1} R_{(j)} - \sum_{i'=i+1}^{m+1} R_{(i')} \\ &= \frac{m-i+1}{m} \sum_{j=1}^{i} R_{(j)} - \frac{i-1}{m} \sum_{j=i+1}^{m+1} R_{(j)}. \end{aligned} \tag{76}$$

  So according to (73), the optimal x_i can be calculated as

$$\begin{aligned} x_i^* &= \frac{1}{m(i-1)} \Bigg(m \sum_{j=1}^{i-1} R_{(j)} - m(i-2)R_{(i)} \\ &\quad - (m-i+1) \sum_{j=1}^{i} R_{(j)} + (i-1) \sum_{j=i+1}^{m+1} R_{(j)} \Bigg) \\ &= \frac{1}{m(i-1)} \Bigg((i-1) \sum_{j=1}^{i-1} R_{(j)} - [m(i-2) \\ &\quad + m - i + 1] R_{(i)} + (i-1) \sum_{j=i+1}^{m+1} R_{(j)} \Bigg) \\ &= \frac{\sum_{j=1}^{i-1} R_{(j)} - (m-1)R_{(i)} + \sum_{j=i+1}^{m+1} R_{(j)}}{m} \\ &= \frac{\sum_{j=1}^{m+1} R_{(j)}}{m} - R_{(i)}. \end{aligned} \tag{77}$$

Therefore, $x_i^* = \frac{\sum_{j=1}^{m+1} R_{(j)}}{m} - R_{(i)}$ has been proved for $3 \le i \le m+1$. Then, according to (24),

$$\begin{aligned} x_2^* &= R_{(1)} - \sum_{i=3}^{m+1} \left(\frac{\sum_{j=1}^{m+1} R_{(j)}}{m} - R_{(i)} \right) \\ &= R_{(1)} - \frac{m-1}{m} \sum_{j=1}^{m+1} R_{(j)} + \sum_{i=3}^{m+1} R_{(i)} \\ &= \frac{R_{(1)} + \sum_{j=3}^{m+1} R_{(j)}}{m} - \frac{m-1}{m} R_{(2)} \\ &= \frac{\sum_{j=1}^{m+1} R_{(j)}}{m} - R_{(2)}. \end{aligned} \tag{78}$$

According to (23), x_1^* can be obtained

$$\begin{aligned} x_1^* = \min \Bigg\{ & \frac{\sum_{j=1}^{m+1} R_{(j)}}{m} - R_{(1)}, R_{(m+2)} - R_{(1)}, \\ & \cdots, R_{(M)} - R_{(1)} \Bigg\} = \frac{\sum_{j=1}^{m+1} R_{(j)}}{m} - R_{(1)}, \end{aligned} \tag{79}$$

where the last relationship holds, since the case in (74) is considered here.

Now, one can verify that $x_i^* \ge 0$ for $\forall i \in \{1, \cdots, M\}$ since the case in (74) is considered. So this solution satisfies the condition in (72), and the optimal value of the objective function is $R_{of}^* = \frac{\sum_{j=1}^{m+1} R_{(j)}}{m}$.

On the other hand, consider the second case $\frac{\sum_{j=1}^{m+1} R_{(j)}}{m} > R_{(m+2)}$. When $m < M-2$, we set

$$x_{m+2} = \frac{\sum_{j=1}^{m+1} R_{(j)} - mR_{(m+2)} - \sum_{i=m+3}^{M} x_m}{m+1}, \tag{80}$$

and then go to step $m+1$. When $m = M-2$, x_M can be calculated as

$$x_M^* = \frac{\sum_{j=1}^{M} R_{(j)}}{M-1} - R_{(M)}. \tag{81}$$

Then, for $i = 1, \cdots, M-1$,

$$x_i^* = \frac{\sum_{j=1}^{M} R_{(j)}}{M-1} - R_{(i)} \tag{82}$$

can be obtained following similar inductive derivations from (76) to (79). Hence $R_{of}^* = \frac{\sum_{j=1}^{M} R_{(j)}}{M-1}$.

Summarizing these $M-2$ steps, Lemma 2 can be proved, and there exist $M-1$ distinct cases as shown in Lemma 2.

REFERENCES

[1] C. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.

[2] A. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, Jan. 1975.

[3] Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2470–2492, 2008.

[4] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Transactions on Information Theory*, vol. 54, no. 10, pp. 4687–4698, 2008.

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

[6] A. Mukherjee, S. A. Fakoorian, J. Huang, and A. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 3, pp. 1550–1573, 2014.

[7] 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.

[8] R. Ahlswede and I. Csiszar, "Common randomness in information theory and cryptography. Part I: secret sharing," *IEEE Transactions on Information Theory*, vol. 39, no. 4, 1993.

[9] I. Csiszár 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.

[10] ——, "Secrecy capacities for multiple terminals," *IEEE Trans. Information Theory*, vol. 50, no. 12, pp. 3047–3061, 2004.

[11] C. Ye and A. Reznik, "Group secret key generation algorithms," in *IEEE International Symposium on Information Theory*, 2007, pp. 2596–2600.

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

[13] S. Nitinawarat and P. Narayan, "Perfect omniscience, perfect secrecy, and steiner tree packing," *IEEE Transactions on Information Theory*, vol. 56, no. 12, pp. 6490–6500, 2010.

[14] L. Lai and S.-W. Ho, "Simultaneously generating multiple keys and multi-commodity flow in networks," in *IEEE Information Theory Workshop (ITW)*, 2012, pp. 627–631.

[15] 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. Information Theory*, vol. 60, no. 10, pp. 6389–6398, Oct 2014.

[16] R. Wilson, D. Tse, and R. A. Scholtz, "Channel identification: Secret sharing using reciprocity in ultrawideband channels," *IEEE Transactions on Information Forensics and Security*, vol. 2, no. 3, pp. 364–375, 2007.

[17] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. B. Mandayam, "Information-theoretically secret key generation for fading wireless channels," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 2, pp. 240–254, 2010.

[18] A. Khisti, "Interactive secret key generation over reciprocal fading channels," in *IEEE 50th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, 2012, pp. 1374–1381.

[19] L. Lai, Y. Liang, and H. V. 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.

[20] L. Lai, Y. Liang, and W. Du, "Phy-based cooperative key generation in wireless networks," in *49th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, Allerton House, UIUC, Illinois, USA, Sept. 2011, pp. 662–669.

[21] ——, "Cooperative key generation in wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 8, pp. 1578–1588, 2012.

[22] 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.

[23] J. Sun, X. Chen, J. Zhang, Y. Zhang, and J. Zhang, "Synergy: A game-theoretical approach for cooperative key generation in wireless networks," in *IEEE INFOCOM*, Toronto, Canada, Apr. 2014, pp. 997–1005.

[24] B. T. Quist and M. A. Jensen, "Maximizing the secret key rate for informed radios under different channel conditions," *IEEE Transactions on Wireless Communications*, vol. 12, no. 10, pp. 5146–5153, 2013.

[25] ——, "Bound on the key establishment rate for multi-antenna reciprocal electromagnetic channels," *IEEE Transactions on Antennas and Propagation*, vol. 62, no. 3, pp. 1378–1385, 2014.

[26] R. Mehmood, J. Wallace, and M. Jensen, "Key establishment employing reconfigurable antennas: Impact of antenna complexity," *IEEE Transactions on Wireless Communications*, vol. 13, no. 11, pp. 6300–6310, Nov 2014.

[27] D. Tse and P. Viswanath, *Fundamentals of wireless communication*. Cambridge university press, 2005.

[28] Q. Wang, H. Su, K. Ren, and K. Kim, "Fast and scalable secret key generation exploiting channel phase randomness in wireless networks," in *IEEE INFOCOM*, 2011, pp. 1422–1430.

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

[30] H. Liu, J. Yang, Y. Wang, Y. Chen, and C. Koksal, "Group secret key generation via received signal strength: Protocols, achievable rates, and implementation," *IEEE Transactions on Mobile Computing*, vol. 13, no. 12, pp. 2820–2835, 2014.

[31] M. Grant and S. Boyd, "CVX: Matlab software for disciplined convex programming," *Optimization Methods and Software*, Apr. 2012, available [online]: http://stanford.edu/∼boyd/cvx.

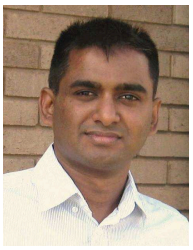
[32] J. Lofberg, "Yalmip: A toolbox for modelling and optimizationin MATLAB," in *Proc. IEEE Int. Symp. on Comp. Aided Control Sys. Design*, Taipei, Sept. 2004, pp. 284–289.

[33] S. Boyd, S. J. Kim, L. Vandenberghe, and A. Hassibi, "A tutorial on geometric programming," *Optimization and Engineering*, vol. 8, no. 1, pp. 67–127, 2007.

[34] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, UK: Cambridge University Press, 2004.

[35] B. R. Marks and G. P. Wright, "A general inner approximation algorithm for nonconvex mathamatical programs," *Operations Research*, vol. 26, no. 4, pp. 681–683, 1978.

Peng Xu received the B.Eng. and the Ph.D. degrees in electronic and information engineering from the University of Science and Technology of China, Anhui, China, in 2009 and 2014, respectively. Since July 2014, he has been working as a postdoctoral researchers with the Department of Electronic Engineering and Information Science, University of Science and Technology of China, Hefei, China. His current research interests include cooperative communications, information theory, information-theoretic secrecy, and 5G networks. He received IEEE Wireless Communications Letters Exemplary Reviewer 2015.

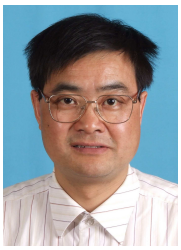


Kanapathippillai Cumanan received the BSc degree with first class honors in electrical and electronic engineering from the University of Peradeniya, Sri Lanka in 2006 and the PhD degree in signal processing for wireless communications from Loughborough University, Loughborough, UK, in 2009.

He is currently a lecturer at the Department of Electronics, University of York, UK. From March 2012 to November 2014, he was working as a research associate at School of Electrical and Electronic Engineering, Newcastle University, UK. Prior to this, he was with the School of Electronic, Electrical and System Engineering, Loughborough University, UK. In 2011, he was an academic visitor at Department of Electrical and Computer Engineering, National University of Singapore, Singapore. From January 2006 to August 2006, he was a teaching assistant with Department of Electrical and Electronic Engineering, University of Peradeniya, Sri Lanka. His research interests include physical layer security, cognitive radio networks, relay networks, convex optimization techniques and resource allocation techniques.

Dr. Cumanan was the recipient of an overseas research student award scheme (ORSAS) from Cardiff University, Wales, UK, where he was a research student between September 2006 and July 2007.

Zhiguo Ding (S'03-M'05-SM'15) received his B.Eng in Electrical Engineering from the Beijing University of Posts and Telecommunications in 2000, and the Ph.D degree in Electrical Engineering from Imperial College London in 2005. From Jul. 2005 to Aug. 2014, he was working in Queens University Belfast, Imperial College and Newcastle University. Since Sept. 2014, he has been with Lancaster University as a Chair Professor. From Oct. 2012 to Sept. 2016, he has been also with Princeton University as an Academic Visitor. Dr Ding's research interests are 5G networks, game theory, cooperative and energy harvesting networks and statistical signal processing. He is serving as an Editor for *IEEE Transactions on Communications*, *IEEE Transactions on Vehicular Networks*, *IEEE Wireless Communication Letters*, *IEEE Communication Letters*, and *Journal of Wireless Communications and Mobile Computing*. He received the best paper award in IET Comm. Conf. on Wireless, Mobile and Computing, 2009, IEEE Communication Letter Exemplary Reviewer 2012, and the EU Marie Curie Fellowship 2012-2014.



Xuchu Dai received the B.Eng. degree in Electrical Engineering in 1984 from Airforce Engineering University, Xi'an, China, the M.Eng. degree in 1991 and the Ph.D. degree in 1998 from University of Science and Technology of China, Hefei, China, both in Communication and Information System.

He now is a Professor with the Department of Electronic Engineering and Information Science, University of Science and Technology of China, Hefei, China. From 2000 to 2002, he was with Hong Kong University of Science and Technology as a postdoctoral researcher. His current research interests include wireless communication systems, blind adaptive signal processing and signal detection.

Kin K. Leung received his B.S. degree from the Chinese University of Hong Kong in 1980, and his M.S. and Ph.D. degrees from University of California, Los Angeles, in 1982 and 1985, respectively.

He joined AT&T Bell Labs in New Jersey in 1986 and worked at its successors, AT&T Labs and Lucent Technologies Bell Labs, until 2004. Since then, he has been the Tanaka Chair Professor in the Electrical and Electronic Engineering (EEE), and Computing Departments at Imperial College in London. He is the Head of Communications and Signal Processing Group in the EEE Department. His current research focuses on protocols, optimization and modeling of various wireless networks. He also works on multi-antenna and cross-layer designs for these networks.

He received the Distinguished Member of Technical Staff Award from AT&T Bell Labs (1994), and was a co-recipient of the Lanchester Prize Honorable Mention Award (1997). He was elected an IEEE Fellow (2001), received the Royal Society Wolfson Research Merits Award (2004-09) and became a member of Academia Europaea (2012). Along with his co-authors, he received several best paper awards, including the IEEE PIMRC 2012 and ICDCS 2013. He has actively served on and led conference committees, including the IEEE SECON 2016 and the ITC 28 (2016). He served as a member (2009-11) and the chairman (2012-15) of the IEEE Fellow Evaluation Committee for Communications Society. He was a guest editor for the IEEE JSAC, IEEE Wireless Communications and the MONET journal, and as an editor for the JSAC: Wireless Series, IEEE Transactions on Wireless Communications and IEEE Transactions on Communications. Currently, he is an editor for the ACM Computing Survey and International Journal on Sensor Networks.