CHINA COMMUNICATIONS

Physical-layer Secret Key Generation for Dual-task Scenarios

Lilin Yang[1], Li Guyue[1,2,*], Guo Tao[1], Xu Hao[3], Hu Aiqun[2,4]

[1] School of Cyber Science and Engineering, Southeast University, Nanjing 210096, China
[2] Purple Mountain Laboratories, Nanjing 210096, China
[3] Department of Electronic and Electrical Engineering, University College London, London WC1E 7JE, UK
[4] National Mobile Communications Research Laboratory, Southeast University, Nanjing 210096, China
[*] The corresponding author, email: guyuelee@seu.edu.cn

Cite as: L. Yang, G. Li, *et al.*, "Physical-layer secret key generation for dual-task scenarios," *China Communications*, 2024, vol. 0, no. 0, pp. 1-13. **DOI**: 10.23919/JCC.YYYY.MM.NNN

Abstract: Physical-layer secret key generation (PSKG) provides a lightweight way for group key (GK) sharing between wireless users in large-scale wireless networks. However, most of the existing works in this field consider only group communication. For a commonly dual-task scenario, where both GK and pairwise key (PK) are required, traditional methods are less suitable for direct extension. For the first time, we discover a security issue with traditional methods in dual-task scenarios, which has not previously been recognized. We propose an innovative segment-based key generation method to solve this security issue. We do not directly use PK exclusively to negotiate the GK as traditional methods. Instead, we generate GK and PK separately through segmentation which is the first solution to meet dual-task. We also perform security and rate analysis. It is demonstrated that our method is effective in solving this security issue from an information-theoretic perspective. The rate results of simulation are also consistent with the our rate derivation.

Keywords: dual-task scenario; information-theoretic security; physical layer security; secret group key generation

Received:
Revised:
Editor:

I. INTRODUCTION

With the development of communication technology, more and more low power terminal scenarios are emerging, such as Wireless Local Area Network (WLAN), Wireless Sensor Network (WSN), Vehicle Networking, etc [1–3]. These networks are currently protected by modern cryptography, including public key cryptography and symmetric encryption [4]. Although these approaches are already quite sophisticated, quantum computers are likely to challenge them in the future. In addition, the dynamic topology and terminal mobility of these networks make it challenging to establish a critical distribution and management center [5, 6].

Recently, Physical-layer Secret Key Generation (PSKG) has received a lot of attention. It is an attractive approach for constructing symmetric encryption in wireless communication networks [7, 8]. Currently, many studies on point-to-point (P2P) scenarios to generate the pairwise key (PK) between two legitimate users are underway [9–14]. Two legitimate communication users take advantage of the inherent randomness in reciprocal wireless channels to share their common key. Furthermore, considering the requirements of secure group communication in large-scale wireless networks, many researchers extend PSKG to generate the group key (GK) with star, ring, and mesh networks [1, 15–21]. To generate GK in these scenarios, common data must be shared among group users.

This is a challenge because the reciprocity assumption holds only between two users [8, 22]. To meet this challenge, many studies have focused on using PK between each pair of users to further negotiate GK [19–21, 23]. For instance, Wei *et al.* [20] use PK in two-user communication to construct the GK, and the central user then uses the XOR algorithm to distribute the GK to other users. In the work of Liu *et al.* [24], the central user calculates DOSS values between a base channel which is designated as the channel from central user to user 1 and other channels, and then broadcasts these DOSS values. In order to obtain the channel quantization result of the base channel, each user subtracts the associated DOSS value, which is used as the shared GK in the network.

Although there are many works on PSKG, their primary focus is on single key generation, where they generate PK in P2P scenarios or GK in multi-user communication scenarios. Few works focus on a commonly seen dual-task scenario where both GK and PK are required and each user in the network should be unaware of any PK between others.

These conventional GK generation schemes are less suitable for dual-task scenarios. For example, in [20], since the GK consists of the PK in two-user communication, users only need to take XOR operation with the GK and messages broadcast on the network to obtain others' PKs. Similarly, utilizing the propagated DOSS values, users in [24] can easily figure out the PK between user 1 and central user by subtracting the propagated DOSS values. This forces the confidentiality of the PK, which should only be privately known by two communicating users for P2P secure communication, to be spread throughout the network. As a result of the spread, a potential attack might occur. In dual-task scenarios, if an attacker with an interest in PK participates honestly in the GK generation, the attacker we described as an inside attacker can obtain other legitimate users' PKs through the GK. As a result, legitimate users' PKs would not be kept private.

In this paper, we propose a novel segment-based key generation scheme that generates not only GK but also PKs, whose confidentiality are not diffused. We elaborate it in star and mesh networks for specific description and analysis. The main contributions of this paper are listed as follows:

- We define an inside attack based on the discovery of the PK confidentiality proliferation problem in dual-task scenarios. Further, we establish a constraint relationship between PK and GK for dual-task.
- We propose a novel segment-based key generation method for dual-task scenarios and employ it to star and mesh networks. We demonstrate that our method can effectively resist both outside and inside attacks from an information-theoretic perspective.
- We design specific schemes for star and mesh networks based on the goal of improving the performance of GK. And we theoretically analyze the rate relationship between GK and PK. Under PK constraint, our method yields the optimal GK rate for the star network and achieves the optimal multiplexing gain for the mesh network, respectively.
- We simulate the variation of GK rate with signal-to-noise ratio (SNR) and the rate relationship between PK and GK for two networks. The numerical results are in agreement with the theoretical analysis.

The remainder of this paper is organized as follows. We first introduce the channel model, attack model, and key generation principle for dual-task scenarios in Section II. Next, in Section III, we provide a segment-based key generation scheme for the star network, which includes algorithm description, rate discussion, and security analysis. Similarly, we also provide a segment-based key generation scheme for the mesh network in Section IV. Then, numerical results are present in Section V. Finally, Section VI summarizes the paper.

II. SYSTEM MODEL

In this section, we introduce the channel model and attack model in the network. After that, we formulate the principle of key generation for dual-task scenarios.

2.1 Channel Model

This paper investigates a dual-task scenario where the number of users is M ($M \geq 3$). Each user A_i $(i \in [0 : M-1])$ is equipped with a single antenna where the distances between users are beyond half wavelength in TDD system. In the wireless channel, each user A_i sends a pilot signal x_i to other users. The received signals are

$$\begin{aligned} y_{i,j} &= h_{i,j}x_i + n_j, \forall j \in [0:M-1], j \neq i, \\ y_{i,e} &= h_{i,e}x_i + n_e, \end{aligned} \tag{1}$$

where $h_{i,j}$ and $h_{i,e}$ denote the fading channel coefficients from A_i to A_j and an attacker, respectively. n_j and n_e are zero mean additive Gaussian noises with variance δ^2 on user A_j and the attacker, respectively.

In the channel estimation stage, it is worth noting that the distances between each user A_i are beyond half a wavelength. Therefore, $h_{i,j}$ and $h_{i,j'}$ $(j \neq j')$ are independent of each other. For simplicity, we assume that each channel gain is a Gaussian random variable (i.e. $h_{i,j}, h_{j,i} \sim CN(0, \delta_{i,j}^2)$) and the channels between user A_i and user A_j are reciprocal (i.e., $h_{i,j} = h_{j,i}$). They remain constant for N symbols and change randomly at the beginning of the next N. Suppose that user A_i broadcasts $\boldsymbol{X}_i$ within N_i symbols in each N, from which user A_j obtains estimated value $\tilde{h}_{i,j}, \forall j \neq i$. According to [19], user A_i and user A_j perform channel estimation and obtain the following estimates:

$$\tilde{h}_{j,i} = h_{j,i} + \frac{\boldsymbol{X}_j^T}{\|\boldsymbol{X}_j\|^2}\boldsymbol{n_i}, \; \tilde{h}_{i,j} = h_{i,j} + \frac{\boldsymbol{X}_i^T}{\|\boldsymbol{X}_i\|^2}\boldsymbol{n_j}. \tag{2}$$

The corresponding energy is defined as $\|\boldsymbol{X}_i\|^2 = N_iP$. All users transmit the signal with the same power constraint P.

After that, user A_i and user A_j can agree on an almost uniformly distributed initial key $\boldsymbol{k}_{i,j} = \boldsymbol{k}_{j,i}$ with arbitrarily small error probability via Slepian-Wolf coding [11, 25, 26]. Note that these initial key $\boldsymbol{k}_{i,j}, i, j \in [0:M-1]$ are mutually independent, i.e.,

$$\begin{aligned} &H(\boldsymbol{k}_{0,1}\boldsymbol{k}_{0,2}\ldots\boldsymbol{k}_{M-2,M-1}) \\ =&H(\boldsymbol{k}_{0,1}) + H(\boldsymbol{k}_{0,2}) + \cdots + H(\boldsymbol{k}_{M-2,M-1}). \end{aligned} \tag{3}$$

In addition, different methods have been investigated to reduce the auto-correlation among channel measurements [27–29]. Therefore, we assume that there is no auto-correlation in these initial keys. After generating initial keys, users exchange messages in a noiseless public channel with infinite capacity which is widely used in existing works [30, 31], and further generate GK and PKs.

2.2 Attack Model

Two types of attackers are considered in this paper. Figure 1 and figure 4 show system models for star and mesh networks, respectively.

- **An Outside Attacker.** This attacker is passive, meaning that it only receives from public and wireless channels and does not send any information. Note that the distances between itself and legitimate users are more than half a wavelength where $h_{i,j}$ and $h_{i,e}$ obtained in the wireless channel are not correlated. Therefore, this attacker's goal is to recover GK and PKs using public channel information.

- **An Inside Attacker.** This attacker is not only interested in GK but also in other legitimate users' PKs. It is a member of a group that participates honestly in GK generation without information tampering, so it can obtain GK in the group, PKs of it own, and messages over the public channel. The goal of this attacker is to recover other legitimate users' PKs through all messages it has mastered. A specific case is described below. Wei *et al.* [20] explained the specific procedure of the GK generation algorithm for a star network under a single cluster. After channel detection, quantization, information negotiation and privacy amplification, each user A_i obtained a shared initial key $\boldsymbol{k}_{i,0}$ with central user A_0. Central user generated $\boldsymbol{K}_G$, which was the result of the XOR operation by initial keys, (i.e. $\boldsymbol{K}_G = \boldsymbol{k}_{1,0} \oplus \boldsymbol{k}_{2,0} \cdots \oplus \boldsymbol{k}_{M-1,0}$). Then, central user broadcast $\boldsymbol{K}_G \oplus \boldsymbol{k}_{i,0}$, for which user A_i obtained $\boldsymbol{K}_G$. Since any user could obtain $\boldsymbol{k}_{i,0}$ by $\boldsymbol{K}_G$ (i.e. $\boldsymbol{k}_{i,0} = (\boldsymbol{K}_G \oplus \boldsymbol{k}_{i,0}) \oplus \boldsymbol{K}_G$) , there was a potential threat that PKs of other legitimate users were leaked to user A_e where user A_e was an inside attacker.

2.3 Key Generation Principle for Dual-task Scenarios

Different from the typical key generation scenario, dual-task scenarios primarily accomplish two tasks: PK generation between any two legitimate users and GK generation in the network. If traditional GK generation methods are applied directly to dual-task scenarios, PKs suffer from an inside attacker as described in Section 2.2. To better describe dual-task scenarios, we formulate the principle of key generation.

Let $\boldsymbol{F}$ denote all messages transmitted over the public channel, f denote the GK generation function (i.e. $\boldsymbol{K}_G = f(\boldsymbol{k}_{i,j}, \boldsymbol{F}), i, j \in [0 : M-1]$), g denote the PK generation function between user A_i and user A_j (i.e. $\boldsymbol{K}_{i,j} = g(\boldsymbol{k}_{i,j})$). Symmetrically, $\boldsymbol{K}_{j,i} = \boldsymbol{K}_{i,j}$. The GK obtained by an attacker is represented as $\boldsymbol{K}_G^e$, and PK obtained by an attacker is $\boldsymbol{K}_{i,j}^e$. The following initial key rate $R_{i,j}$ is shown in [19] to be achievable:

$$\begin{aligned} R_{i,j} &= I(\tilde{h}_{i,j}; \tilde{h}_{j,i})/N \\ &= -\frac{1}{2} log(1 - \frac{1}{(1+\frac{\delta^2}{\delta_{i,j}^2 PN_j})(1+\frac{\delta^2}{\delta_{i,j}^2 PN_i})})/N, \end{aligned} \tag{4}$$

where $cov(\tilde{h}_{i,j},\tilde{h}_{j,i}) = \delta_{i,j}^2$, $var(\tilde{h}_{i,j}) = \delta_{i,j}^2 + \frac{\delta^2}{\|\boldsymbol{X}_i\|^2}$, and $var(\tilde{h}_{j,i}) = \delta_{i,j}^2 + \frac{\delta^2}{\|\boldsymbol{X}_j\|^2}$. The above key rate can be implemented on the basis of Slepian-Wolf coding and additional transmission over the public channel [11]. In the sequel, we need to achieve error-free transmission over the public noiseless channel, and this can be achieved by error correction coding.

For any $\epsilon > 0$,

$$\begin{aligned} &Pr(\boldsymbol{K}_{j,i} \neq \boldsymbol{K}_{i,j}) < \epsilon, \\ &Pr(\boldsymbol{K}_{i,j} = \boldsymbol{K}_{i,j}^e) < \epsilon, \\ &Pr(\boldsymbol{K}_G^i \neq \boldsymbol{K}_G^j) < \epsilon, \\ &\frac{1}{N} H(\boldsymbol{K}_{i,j}) > R_P^{i,j} - \epsilon, \\ &\frac{1}{N} H(\boldsymbol{K}_G) > R_G - \epsilon, \end{aligned} \tag{5}$$

where $R_P^{i,j}$ and R_G denote the achievable PK rate and GK rate, respectively.

III. SEGMENT-BASED KEY GENERATION IN THE STAR NETWORK

This section provides the segment-based key generation scheme in the star network which consists of PK generation and GK generation. The central user is denoted as A_0 and the remaining users are denoted as A_i, $i \in [1 : M-1]$. $\boldsymbol{K}_{i,0}$ and $\boldsymbol{K}_G^*$ denote the PK between user A_i and user A_0 and GK in the star network, respectively. An outside attacker and an inside attacker exist as shown in figure 1.

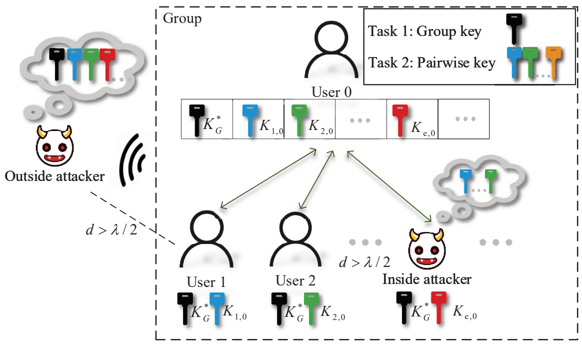


Figure 1. *The system model in the star network.*

Algorithm 1. *Segment-based key generation algorithm in the star network.*

```
Input: $\boldsymbol{k}_{i,0}$
Output: $\boldsymbol{K}_G^*$ and $\boldsymbol{K}_{i,0}$
for each $A_i, i \in [0 : M-1]$ do
    $\boldsymbol{k}_{i,0} = (\boldsymbol{k}_{i,0}^1, \boldsymbol{k}_{i,0}^2), i \in [1 : M-1]$
    $\boldsymbol{K}_{i,0} = g(\boldsymbol{k}_{i,0}^2)$
end for
$\boldsymbol{k}_{i^*,0}^1 = \boldsymbol{k}_{1,0}^1 \wedge \boldsymbol{k}_{2,0}^1 \wedge \cdots \wedge \boldsymbol{k}_{M-1,0}^1$
for Time = 1 to $M-2$ do
    $A_0$ broadcasts $\boldsymbol{k}_{i^*,0}^1 \oplus \boldsymbol{k}_{i,0}^1, i \in [1 : M-1], i \neq i^*$
end for
for each $A_i, i \in [0 : M-1]$ do
    $\boldsymbol{K}_G^* = \boldsymbol{k}_{i^*,0}^1, i^* \in [1 : M-1]$
end for
```

3.1 Key Generation Algorithm

It is known that $\boldsymbol{k}_{i,0}$ obtained by user A_i is consistent with the $\boldsymbol{k}_{0,i}$ obtained by central user A_0, i.e., $\boldsymbol{k}_{i,0} = \boldsymbol{k}_{0,i}$. Therefore, we have $R_{i,0} = R_{0,i}$. From 1-1 to 1-2, we describe the PK generation. And then, we accomplish the GK generation from 2-1 to 2-2. The complete algorithm is shown in Algorithm 1.

1-1. Each user $A_i, i \in [0 : M-1]$ segments its initial keys $\boldsymbol{k}_{i,0}, i \in [1 : M-1]$ into two independent part $\boldsymbol{k}_{i,0}^1$ and $\boldsymbol{k}_{i,0}^2$ by means of a one-to-one mapping: $\mathcal{K}_{i,0} \to \mathcal{K}_{i,0}^1 \times \mathcal{K}_{i,0}^2$ as shown in figure 2. Note that all users including attackers know the mapping criteria. Then, in terms of the achievable rate we have

$$R_{i,0} = R_{i,0}^1 + R_{i,0}^2, \tag{6}$$

where $R_{i,0}^1$ and $R_{i,0}^2$ represent the rate of $\boldsymbol{k}_{i,0}^1$ and $\boldsymbol{k}_{i,0}^2$, respectively. Moreover, due to independent

Table 1. *Definition of partial notations.*

Notation	Definition
M	Number of users
$A_i, i \in [0 : M-1]$	Legitimate users, A_0 for central user in the star network
$\boldsymbol{k}_{i,j}$	Shared initial key for user A_i and user A_j
$\boldsymbol{k}^1_{i,0}, \boldsymbol{k}^2_{i,0}, i \in [1 : M-1]$	Segments of the initial key $\boldsymbol{k}_{i,0}$ in the star network
$\boldsymbol{K}_G$	Group key (GK)
$\boldsymbol{K}^*_G$	GK in the star network
$\boldsymbol{K}^{mesh}_G$	GK in the mesh network
$\boldsymbol{K}^e_G$	GK obtained by attacker
$\boldsymbol{K}_{i,j}$	Pairwise key (PK) between user A_i and user A_j
$\boldsymbol{K}^e_{i,j}$	PK between user A_i and user A_j obtained by attacker
$\boldsymbol{F}$	All messages in public channel
$R_{i,j}$	The rate of $\boldsymbol{k}_{i,j}$
R_G	The rate of $\boldsymbol{K}_G$
R^*_G	The rate of $\boldsymbol{K}^*_G$
R^{mesh}_G	The rate of $\boldsymbol{K}^{mesh}_G$
$R^{i,j}_P$	The rate of $\boldsymbol{K}_{i,j}$
$\sum_{j=0,j\neq i}^{M-1} R^{i,j}_P$	sum rate of $\boldsymbol{K}_{i,j}$ for user A_i

segments, we have

$$I(\boldsymbol{k}^1_{i,0}; \boldsymbol{k}^2_{i,0}) = 0, i \in [1 : M-1]. \tag{7}$$

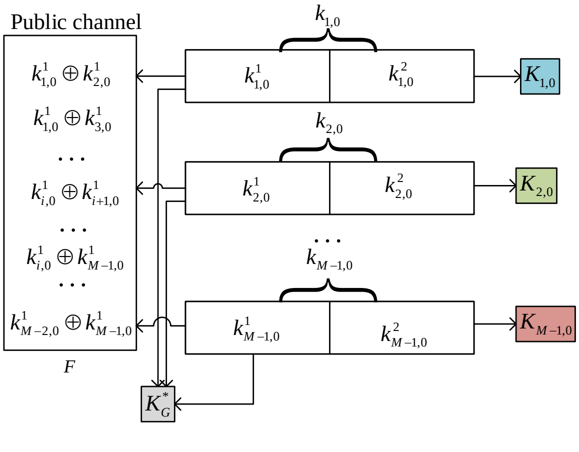


Figure 2. *The segment diagram in the star network.*

1-2. The $\boldsymbol{k}^2_{i,0}$ part is used as the input of user A_i's PK generation function, i.e., $\boldsymbol{K}_{i,0} = g(\boldsymbol{k}^2_{i,0}), i \in [1 : M-1]$. Thus,

$$H(\boldsymbol{K}_{i,0}) \leq H(\boldsymbol{k}^2_{i,0}), \tag{8}$$

and the PK rate is

$$R^{i,0}_P \leq R^2_{i,0}. \tag{9}$$

2-1. Central user A_0 first selects $\boldsymbol{k}^1_{i^*,0}$ which has the shortest length $|\boldsymbol{k}^1_{i^*,0}|$ among $\boldsymbol{k}^1_{i,0}, i = [1 : M-1]$, denoted as $\boldsymbol{k}^1_{i^*,0} = \boldsymbol{k}^1_{1,0} \wedge \boldsymbol{k}^1_{2,0} \wedge \cdots \wedge \boldsymbol{k}^1_{M-1,0}$. After that, central user A_0 broadcasts $\boldsymbol{k}^1_{i^*,0} \oplus \boldsymbol{k}^1_{i,0}, i \in [1 : M-1], i \neq i^*$ in the public channel, where error-free transmission can be realized by a channel coding. Here, we omit the details of channel coding. $\boldsymbol{F}$ denotes all messages over the public channel, i.e.,

$$\begin{aligned} \boldsymbol{F} &= \mu(\boldsymbol{k}^1_{1,0}, \ldots, \boldsymbol{k}^1_{M-1,0}) \\ &= (\boldsymbol{k}^1_{i^*,0} \oplus \boldsymbol{k}^1_{i,0}, i \in [1 : M-1], i \neq i^*). \end{aligned} \tag{10}$$

2-2. After broadcasting $M-2$ messages, all users obtain $\boldsymbol{k}^1_{i^*,0}, i^* \in [1 : M-1]$ to form the GK. The GK rate is

$$R^*_G = \min_{1 \leq i \leq M-1} R^1_{i,0}. \tag{11}$$

3.2 The Key Rate of PK and GK

Let $\mathcal{R}^*_{dual-task}$ be the region of all achievable rate pairs $(R^*_G, R^{i,0}_P)$ for the star network. In the following Lemma 1 and 2, we specifically investigate the scope of $\mathcal{R}^*_{dual-task}$ in dual-task scenarios.

Lemma 1. *According to Algorithm 1, the region of our scheme can be expressed as*

$$\begin{aligned}&\mathcal{R}^*_{dual-task} = \bigcup\{(R^*_G, R^{i,0}_P):\\&0 \le R^*_G \le R_{min},\\&0 \le R^{i,0}_P \le R_{i,0},\\&0 \le R^{i,0}_P + R^*_G \le R_{i,0}\},\end{aligned} \tag{12}$$

where $R_{min} = \min_{1\le i\le M-1}\{R_{i,0}\}$. *The region enclosed by $A-B-D-O-A$ in figure 3 represents it.*

Further, a rate-constrained case is considered that there are constraints on the rate of $\boldsymbol{K}_{i,0}$. We denote as $R^{i,0}_P \ge \alpha$, where $0 < \alpha < R_{min}$.

Lemma 2. *The region in the rate-constrained case becomes*

$$\begin{aligned}&\mathcal{R}^*_{dual-task} = \bigcup\{(R^*_G, R^{i,0}_P):\\&0 \le R^*_G \le R'_{min},\\&\alpha \le R^{i,0}_P \le R_{i,0},\\&0 \le R^{i,0}_P + R^*_G \le R_{i,0}\},\end{aligned} \tag{13}$$

where $R'_{min} = \min_{1\le i\le M-1}\{R_{i,0} - \alpha\}$.

Remark 1. *When user A_m has $R_{m,0} - \alpha > R'_{min}$, $\mathcal{R}^*_{dual-task}$ is surrounded by $G-C-D-F-G$ in figure 3, and it is enclosed by $H-D-F-H$ when $R_{m,0} - \alpha = R'_{min}$.*

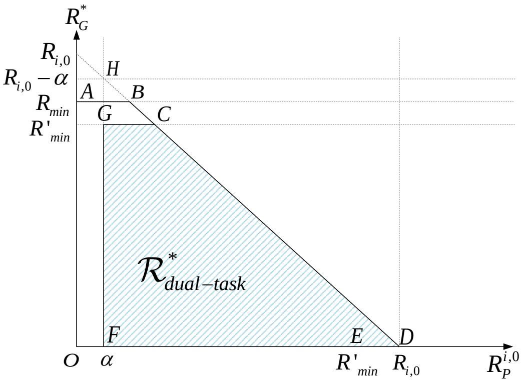


Figure 3. *The key rate region between PK and GK in the star network.*

Proposition 1. *With constraints on $R^{i,0}_P$, R^*_G obtained by Algorithm 1 achieves the optimal GK rate when $H(\boldsymbol{K}_{i,0}) = H(\boldsymbol{k}^2_{i,0})$.*

Proof. In the star network, the upper bound within constraints on PK for achievable GK rate in [21] is

$$R^{upper,*}_G = \min_{1\le i\le M-1}\{R_{i,0} - R^{i,0}_P\}. \tag{14}$$

In view of Eq.(6), Eq.(9) and Eq.(11), the achievable GK rate in our method is

$$R^*_G = \min_{1\le i\le M-1}\{R_{i,0} - R^2_{i,0}\} \le \min_{1\le i\le M-1}\{R_{i,0} - R^{i,0}_P\}. \tag{15}$$

Only when $H(\boldsymbol{K}_{i,0}) = H(\boldsymbol{k}^2_{i,0})$, we have $R^*_G = R^{upper,*}_G$. When the demand of PK is small, i.e., $H(\boldsymbol{K}_{i,0}) < H(\boldsymbol{k}^2_{i,0})$, the GK rate is affected by PK which cannot achieve the optimal.

3.3 Security Analysis

According to Section 2.2, attackers can be divided into two categories. Specifically, we perform security analysis based on the purpose of two attackers. The following theorems state that our method is secure in the star network.

Theorem 1. ***(Outside Attack)*** *$\boldsymbol{K}_{i,0}, i \in [1 : M-1]$ and $\boldsymbol{K}^*_G$ are provably secure from an outside attacker who experiences an independent wireless channel from legitimate users.*

Proof. The outside attacker observes $\boldsymbol{F}$ as Eq.(10). According to Eq.(3) and Eq.(8), we obtain

$$\begin{aligned}&I(\boldsymbol{K}_{1,0}, \boldsymbol{K}_{2,0}, \ldots, \boldsymbol{K}_{M-1,0}; \boldsymbol{F})\\&\le I(\boldsymbol{k}^2_{1,0}, \ldots, \boldsymbol{k}^2_{M-1,0}; \mu(\boldsymbol{k}^1_{1,0}, \ldots, \boldsymbol{k}^1_{M-1,0}))\\&=0,\end{aligned} \tag{16}$$

where the final equality is derived from $I(\boldsymbol{k}^2_{1,0}, \ldots, \boldsymbol{k}^2_{M-1,0}; \mu(\boldsymbol{k}^1_{1,0}, \ldots, \boldsymbol{k}^1_{M-1,0})) = 0$.

From Eq.(3) and Eq.(6), we have

$$\begin{aligned}
&I(\boldsymbol{K}_G^*;\boldsymbol{F})\\
=&I(\boldsymbol{k}_{1,0}^1,\boldsymbol{k}_{2,0}^1,\ldots,\boldsymbol{k}_{M-1,0}^1;\boldsymbol{F})-\sum_{j=1,j\neq i^*}^{M-1}H(\boldsymbol{k}_{j,0}^1)\\
=&I(\boldsymbol{k}_{1,0}^1,\boldsymbol{k}_{2,0}^1,\ldots,\boldsymbol{k}_{M-1,0}^1;\boldsymbol{k}_{i^*,0}^1\oplus\boldsymbol{k}_{1,0}^1,\ldots,\boldsymbol{k}_{i^*,0}^1\oplus\boldsymbol{k}_{M-1,0}^1)\\
&-(M-2)H(\boldsymbol{k}_{i^*,0}^1)\\
=&0,
\end{aligned} \tag{17}$$

where the last equality is derived from $I(\boldsymbol{k}_{1,0}^1,\boldsymbol{k}_{2,0}^1,\ldots,\boldsymbol{k}_{M-1,0}^1;\boldsymbol{k}_{i^*,0}^1\oplus\boldsymbol{k}_{1,0}^1,\ldots,\boldsymbol{k}_{i^*,0}^1\oplus\boldsymbol{k}_{M-1,0}^1)\leq H(\boldsymbol{k}_{i^*,0}^1\oplus\boldsymbol{k}_{1,0}^1,\ldots,\boldsymbol{k}_{i^*,0}^1\oplus\boldsymbol{k}_{M-1,0}^1)\leq(M-2)H(\boldsymbol{k}_{i^*,0}^1)$.

Remark 2. *Eq.(16) proves that an outside attacker cannot obtain any information about $\boldsymbol{K}_{i,0}, i\in[1:M-1]$. Eq.(17) proves that an outside attacker cannot obtain $\boldsymbol{K}_G^*$ by public channel information.*

Theorem 2. ***(Inside Attack)*** *$\boldsymbol{K}_{i,0}, i\in[1:M-1], i\neq e$ is provably secure from an inside attacker A_e which is a member of the network.*

Proof. Different from the outside attacker, the inside attacker A_e is able to obtain $\boldsymbol{K}_{e,0}, \boldsymbol{K}_G^*$ and $\boldsymbol{F}$ like other legitimate users. But the goal of the inside attacker is to recover other legitimate users' PKs of the group. Thus, in view of Eq.(3), Eq.(7) and Eq.(8) , we have

$$\begin{aligned}
&I(\boldsymbol{K}_{1,0},\ldots,\boldsymbol{K}_{M-1,0};\boldsymbol{K}_{e,0},\boldsymbol{K}_G^*,\boldsymbol{F})\\
=&I(\boldsymbol{K}_{1,0},\ldots,\boldsymbol{K}_{M-1,0};\boldsymbol{K}_{e,0})\\
&+I(\boldsymbol{K}_{1,0},\ldots,\boldsymbol{K}_{M-1,0};\boldsymbol{K}_G^*,\boldsymbol{F}|\boldsymbol{K}_{e,0})\\
\leq&H(\boldsymbol{k}_{e,0}^2)-I(\boldsymbol{k}_{e,0}^2;\boldsymbol{k}_{i^*,0}^1,\mu(\boldsymbol{k}_{1,0}^1,\ldots,\boldsymbol{k}_{M-1,0}^1))\\
&+I(\boldsymbol{k}_{1,0}^2,\ldots,\boldsymbol{k}_{M-1,0}^2;\boldsymbol{k}_{i^*,0}^1,\mu(\boldsymbol{k}_{1,0}^1,\ldots,\boldsymbol{k}_{M-1,0}^1))\\
\leq&H(\boldsymbol{k}_{e,0}^2).
\end{aligned} \tag{18}$$

Remark 3. *Eq.(18) proves that an inside attacker cannot obtain $\boldsymbol{K}_{i,0}, i\in[1:M-1], i\neq e$ of other legitimate users except itself.*

IV. SEGMENT-BASED KEY GENERATION IN THE MESH NETWORK

This section provides the segment-based key generation scheme in the mesh network. In this network, users are denoted as $A_i,\ i\in[0:M-1]$, $\boldsymbol{K}_G^{mesh}$ and $\boldsymbol{K}_{i,j}$ denote GK and PK, respectively. An outside attacker and an inside attacker exist as shown in figure 4.

Algorithm 2. *Segment-based key generation algorithm in the mesh network.*

```
Input: $\boldsymbol{k}_{i,j}$
Output: $\boldsymbol{K}_G^{mesh}$ and $\boldsymbol{K}_{i,j}$
for each $A_i, i\in[0:M-1]$ do
    $\boldsymbol{k}_{i,j}=(\boldsymbol{k}_{i,j}^{(1)},\boldsymbol{k}_{i,j}^{(2)}), j\neq i$
    $\boldsymbol{K}_{i,j}=g(\boldsymbol{k}_{i,j}^{(2)})$
    $\boldsymbol{k}_{i,j}^{(1)}=(\boldsymbol{k}_{i,j}^{i},\boldsymbol{k}_{i,j}^{j}), j\neq i$
    $\boldsymbol{k}_i^s=\boldsymbol{k}_{i,0}^i\wedge\boldsymbol{k}_{i,1}^i\wedge\cdots\wedge\boldsymbol{k}_{i,M-1}^i$
    $A_i$ broadcasts $\boldsymbol{k}_i^s\oplus\bar{\boldsymbol{k}}_{i,j}^i, j\in[0:M-1], j\neq i$
    $\boldsymbol{K}_G^{mesh}=(\boldsymbol{k}_0^s,\ldots,\boldsymbol{k}_{M-1}^s)$
end for
```

It is worth noting that we segment one more time in the mesh network than in the star network. The first segmentation is to meet dual-task requirements securely like in the star network. But the second segmentation is to improve the performance of the GK which we derive and explain in Proposition 2.

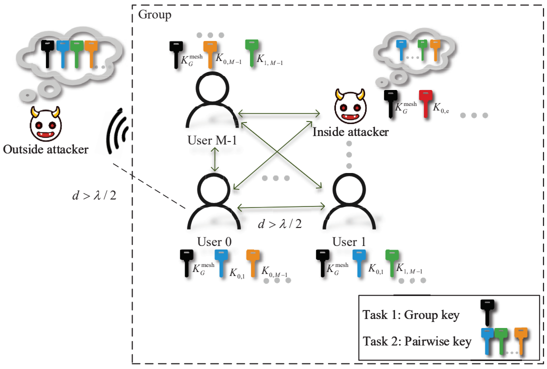


Figure 4. *The system model in the mesh network.*

4.1 Key Generation Algorithm

Similar to Section III, we have $\boldsymbol{k}_{i,j}=\boldsymbol{k}_{j,i}, R_{i,j}=R_{j,i}$. Algorithm 2 shows the complete algorithm.

3-1. Each user $A_i, i\in[0:M-1]$ segments its initial keys $\boldsymbol{k}_{i,j}, j\in[0:M-1], j\neq i$ into independent parts $\boldsymbol{k}_{i,j}^{(1)}$ and $\boldsymbol{k}_{i,j}^{(2)}$ by means of the mapping, we have

$$R_{i,j}=R_{i,j}^{(1)}+R_{i,j}^{(2)}, \tag{19}$$

where $R_{i,j}^{(1)}$ and $R_{i,j}^{(2)}$ represent the rate of $\boldsymbol{k}_{i,j}^{(1)}$ and $\boldsymbol{k}_{i,j}^{(2)}$, respectively. We omit the description of independence formula for convenience.

3-2. The $\boldsymbol{k}_{i,j}^{(2)}$ part is used as the input of PK generation function between user A_i and user A_j, i.e. $\boldsymbol{K}_{i,j} = g(\boldsymbol{k}_{i,j}^{2})$. Total PK rate for user A_i is

$$\sum_{j=0,j\neq i}^{M-1} R_P^{i,j} \leq \sum_{j=0,j\neq i}^{M-1} R_{i,j}^{(2)}. \tag{20}$$

4-1. Each user A_i segments $\boldsymbol{k}_{i,j}^{(1)}$, $j \in [0 : M-1], j \neq i$ into independent parts $\boldsymbol{k}_{i,j}^{i}$ and $\boldsymbol{k}_{i,j}^{j}$, then select $\boldsymbol{k}_i^s$ which has the shortest length $|\boldsymbol{k}_i^s|$ among $\boldsymbol{k}_{i,j}^{i}, j = [0 : M-1]$, i.e. $\boldsymbol{k}_i^s = \boldsymbol{k}_{i,0}^{i} \wedge \boldsymbol{k}_{i,1}^{i} \wedge \cdots \wedge \boldsymbol{k}_{i,M-1}^{i}$, we have

$$\begin{aligned} R_{i,j}^{(1)} &= R_{i,j}^{i} + R_{i,j}^{j}, \\ R_i^s &= \min_{0\leq j\leq M-1, j\neq i} R_{i,j}^{i}, \end{aligned} \tag{21}$$

where $R_{i,j}^{i}$, $R_{i,j}^{j}$ and R_i^s represent the rate of $\boldsymbol{k}_{i,j}^{i}$, $\boldsymbol{k}_{i,j}^{j}$ and $\boldsymbol{k}_i^s$ respectively. Figure 5 gives the detailed segment diagram.

4-2. Each user A_i broadcasts $\boldsymbol{k}_i^s \oplus \bar{\boldsymbol{k}}_{i,j}^{i}, i, j \in [0 : M-1], i \neq j$ in the public channel, where $\bar{\boldsymbol{k}}_{i,j}^{i}$ denotes the first $|\boldsymbol{k}_i^s|$ bits of $\boldsymbol{k}_{i,j}^{i}$. Thus, $\boldsymbol{F} = (\boldsymbol{k}_i^s \oplus \bar{\boldsymbol{k}}_{i,j}^{i}, i, j \in [0 : M-1], i \neq j)$.

4-3. Concatenate all $\boldsymbol{k}_i^s$ to form GK, i.e. $\boldsymbol{K}_G^{mesh} = (\boldsymbol{k}_0^s, \ldots, \boldsymbol{k}_{M-1}^s)$. The GK rate is

$$\begin{aligned} R_G^{mesh} &= \sum_{i=0}^{M-1} R_i^s \\ &= \sum_{i=0}^{M-1} \min_{0\leq j\leq M-1, j\neq i} \{R_{i,j} - R_{i,j}^{(2)} - R_{i,j}^{j}\}. \end{aligned} \tag{22}$$

4.2 The Key Rate of PK and GK

In this subsection, similar to Section 3.2, we define $\mathcal{R}_{dual-task}^{mesh}$ to be the region of all achievable rate pairs $(R_G^{mesh}, \sum_{j=0,j\neq i}^{M-1} R_P^{i,j})$ for the mesh network. In the following Lemma 3 and 4, we specifically investigate the scope of $\mathcal{R}_{dual-task}^{mesh}$ in dual-task scenarios.

Lemma 3. *The region $\mathcal{R}_{dual-task}^{mesh}$ for user A_i can be expressed as Eq.(23), where the region enclosed with $A-B-D-O-A$ in figure 6 shows it.*

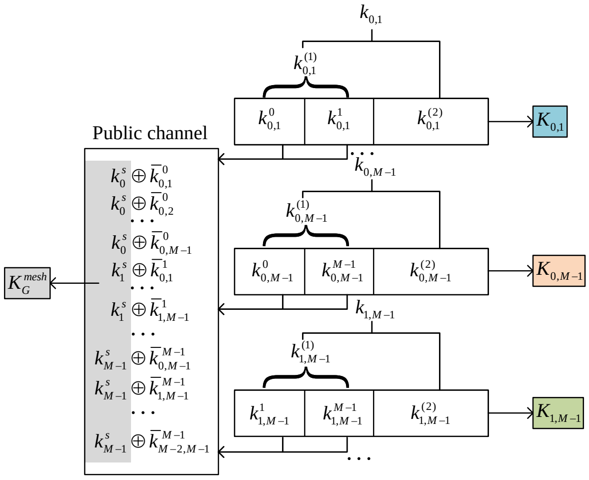

$k_{0,1}$
$k_{0,1}^{(1)}$
$k_{0,1}^{0}$
$k_{0,1}^{1}$
$k_{0,1}^{(2)}$
$K_{0,1}$
Public channel
$k_0^s \oplus \bar{k}_{0,1}^{0}$
$k_0^s \oplus \bar{k}_{0,2}^{0}$
$k_0^s \oplus \bar{k}_{0,M-1}^{0}$
$k_1^s \oplus \bar{k}_{0,1}^{1}$
$k_1^s \oplus \bar{k}_{1,M-1}^{1}$
$k_{M-1}^s \oplus \bar{k}_{0,M-1}^{M-1}$
$k_{M-1}^s \oplus \bar{k}_{1,M-1}^{M-1}$
$k_{M-1}^s \oplus \bar{k}_{M-2,M-1}^{M-1}$
K_G^{mesh}
$k_{0,M-1}$
$k_{0,M-1}^{(1)}$
$k_{0,M-1}^{0}$
$k_{0,M-1}^{M-1}$
$k_{0,M-1}^{(2)}$
$K_{0,M-1}$
$k_{1,M-1}$
$k_{1,M-1}^{(1)}$
$k_{1,M-1}^{1}$
$k_{1,M-1}^{M-1}$
$k_{1,M-1}^{(2)}$
$K_{1,M-1}$

Figure 5. *The segment diagram in the mesh network.*

$$\begin{aligned} \mathcal{R}_{dual-task}^{mesh} &= \bigcup \{ (R_G^{mesh}, R_P^{i,j}) : \\ 0 \leq R_G^{mesh} &\leq \min_{0\leq i\leq M-1} \sum_{j=0,j\neq i}^{M-1} R_{i,j}, \\ 0 \leq \sum_{j=0,j\neq i}^{M-1} R_P^{i,j} &\leq \sum_{j=0,j\neq i}^{M-1} R_{i,j}, \\ 0 \leq R_G^{mesh} + \sum_{j=0,j\neq i}^{M-1} R_P^{i,j} &\leq \sum_{j=0,j\neq i}^{M-1} R_{i,j} \}. \end{aligned} \tag{23}$$

Consider that there is a rate-constrained case as $R_P^{i,j} \geq \beta$, where $0 < \beta < \min_{0\leq i,j\leq M-1, i\neq j} R_{i,j}$.

Lemma 4. *$\mathcal{R}_{dual-task}^{mesh}$ in the rate-constrained case becomes*

$$\begin{aligned} \mathcal{R}_{dual-task}^{mesh} &= \bigcup \{ (R_G^{mesh}, R_P^{i,j}) : \\ 0 \leq R_G^{mesh} &\leq \min_{0\leq i\leq M-1} \{ \sum_{j=0,j\neq i}^{M-1} R_{i,j} - (M-1)\beta \}, \\ (M-1)\beta \leq \sum_{j=0,j\neq i}^{M-1} R_P^{i,j} &\leq \sum_{j=0,j\neq i}^{M-1} R_{i,j}, \\ 0 \leq R_G^{mesh} + \sum_{j=0,j\neq i}^{M-1} R_P^{i,j} &\leq \sum_{j=0,j\neq i}^{M-1} R_{i,j} \}. \end{aligned} \tag{24}$$

Remark 4. *In figure 6, if user A_m has $\sum_{l=0,l\neq m}^{M-1} R_{m,l} = \min_{0\leq i\leq M-1} \sum_{j=0,j\neq i}^{M-1} R_{i,j}$,*

$R_{dual-task}^{mesh}$ is enclosed by $G-D-E-G$. However, if user A_m has $\sum_{l=0,l\neq m}^{M-1} R_{m,l} > \min_{0\le i\le M-1}\sum_{j=0,j\neq i}^{M-1} R_{i,j}$, we discover that even if $\sum_{l=0,l\neq m}^{M-1} R_{m,l}$ increases, $R_{dual-task}^{mesh}$ is also bounded by $\min_{0\le i\le M-1}\sum_{j=0,j\neq i}^{M-1} R_{i,j}$, as the region enclosed by $F-C-D-E-F$.

Proposition 2. *With constraints on $R_P^{i,j}$, Algorithm 2 can achieve the optimal multiplexing gain $\frac{M}{2}$ which is not affected by PKs.*

Proof. In the mesh network, the upper bound within constraints on PK rate for achievable GK rate in [21] is

$$R_G^{upper,mesh} = \min_{0\le i\le M-1} \frac{1}{(M-1)} \min_{(B_0,\ldots,B_{M-1})\in\mathcal{B}_M(\mathcal{A})} \{ \sum_{(i,j):i\in B_l,j\in B_r;l<r} (R_{i,j}-R_P^{i,j})\}. \tag{25}$$

Note that the collection of all M-partitions $(B_0,\ldots,B_{M-1})$ is denoted as $\mathcal{B}_M(\mathcal{A})$. There is only one user in each bin B_l for the M-partitions. The multiplexing gain of the upper bound key rate is defined in [25] as

$$\lim_{P\to\infty} \frac{R_G^{upper,mesh}}{R_s}, \tag{26}$$

where $R_s = logP/N$. Thus

$$\begin{aligned}
&\lim_{P\to\infty} \frac{R_G^{upper,mesh}}{R_s} \\
&= \min_{0\le i\le M-1} \frac{1}{(M-1)} \min_{(B_0,\ldots,B_{M-1})\in\mathcal{B}_M(\mathcal{A})} \{ \\
&\quad \sum_{(i,j):i\in B_l,j\in B_r;l<r} (\lim_{P\to\infty} \frac{R_{i,j}-R_P^{i,j}}{R_s})\} \\
&\le \frac{1}{(M-1)} \sum_{0\le i<j\le M-1} (\lim_{P\to\infty} \frac{R_{i,j}-R_P^{i,j}}{R_s}) \\
&= \frac{M}{2}.
\end{aligned} \tag{27}$$

The result of the last equality is obtained from $\begin{pmatrix} M \\ 2 \end{pmatrix} = \frac{M(M-1)}{2}$ in the mesh network. We set $R_{i,j}^{(2)} = \gamma, R_{i,j}^{i} = R_{i,j}^{j} = (R_{i,j}-\gamma)/2, 0 \le \gamma \le \min_{0\le i,j\le M-1,i\neq j} R_{i,j}, i\neq j \in [0:M-1]$, the multiplexing gain of R_G^{mesh} is

$$\begin{aligned}
\lim_{P\to\infty} \frac{R_G^{mesh}}{R_s} &= \frac{1}{2}\sum_{i=1}^{M} \min_{1\le j\le M,j\neq i} (\lim_{P\to\infty} \frac{R_{i,j}-\gamma}{R_s}) \\
&= \frac{M}{2}.
\end{aligned} \tag{28}$$

Therefore, it is proved that our scheme can achieve the optimal multiplexing gain for GK in dual-task scenarios. By segmenting one more time than the star network, GK in the mesh network achieves the optimal multiplexing gain that segmentation by once could not obtain. Besides, unlike the proof of optimal multiplexing gain in [19], the result indicates that even in dual-task scenarios, PKs generated by the segment-based method do not affect the multiplexing gain of GK. And the multiplexing gain is related to the number of users M and the network. This conclusion is novel. Further, similar to Section 3.3, our method is also provably secure in the mesh network, here we do not describe details.

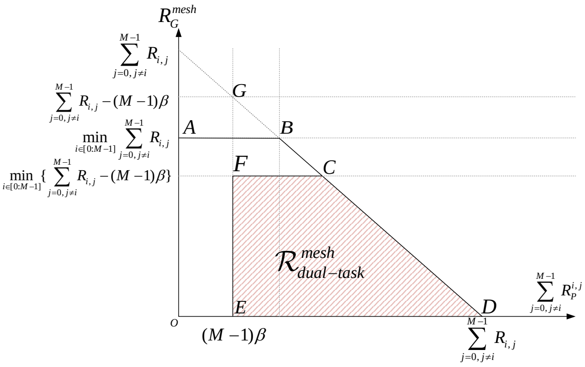

R_G^{mesh}
$\sum_{j=0,j\neq i}^{M-1} R_{i,j}$
$\sum_{j=0,j\neq i}^{M-1} R_{i,j}-(M-1)\beta$
$\min_{i\in[0:M-1]} \sum_{j=0,j\neq i}^{M-1} R_{i,j}$
$\min_{i\in[0:M-1]} \{\sum_{j=0,j\neq i}^{M-1} R_{i,j}-(M-1)\beta\}$
G
A
B
F
C
$\mathcal{R}_{dual-task}^{mesh}$
E
D
o
$(M-1)\beta$
$\sum_{j=0,j\neq i}^{M-1} R_{i,j}$
$\sum_{j=0,j\neq i}^{M-1} R_P^{i,j}$

Figure 6. *The key rate region between PKs and GK in the mesh network.*

V. NUMERICAL RESULTS

In order to validate our theoretical conclusion, we provide some numerical examples in this section. We draft the rate relationship between GK and PK for the star and mesh networks mentioned in this paper. Moreover, we simulate GK rate in both our approach and [21] with constrained PK rate. For simplicity, we set all noise variances to one (i.e. $\delta^2 = 1$), where value of the power P is equal to the signal-to-noise ratio

(SNR), and the number of legitimate users is four (i.e. $M = 4$). Besides, $N_i = 3, i \in \{0, 1, 2, 3\}$, $N = 12$.

In the star network, user A_0 is the central user. Figure 7 plots the rate relationship between PK and GK in the star network, where $(\delta_{1,0}^2, \delta_{2,0}^2, \delta_{3,0}^2) = (2.5, 4, 12)$. Note that, we set $\alpha = 0$ and $R_P^{i,0} = R_{i,0}^2$. When we do not strictly fix $R_P^{i,0}$ (i.e. $R_P^{1,0} = R_P^{2,0} = R_P^{3,0} \geq \alpha$), a clear linear relationship between R_G^* and $R_P^{i,0}$ is shown in figure 7. And this linear relationship is bounded by the minimum channel variance (i.e. $\delta_{1,0}^2 = 2.5$). In addition, when some $R_P^{i,0}$ are fixed, for user A_1, due to $R_{1,0} - \alpha = R'_{min}$, the rate relationship satisfies the triangular region as mentioned in Remark 1, where $R'_{min} = \min_{1 \leq i \leq 3}\{R_{i,0} - \alpha\}$. When $R_{i,0} - \alpha > R'_{min}$, the rate relationship is bounded by R'_{min}. From the numerical results, it could be noticed that the relationship satisfies the Lemma 2.

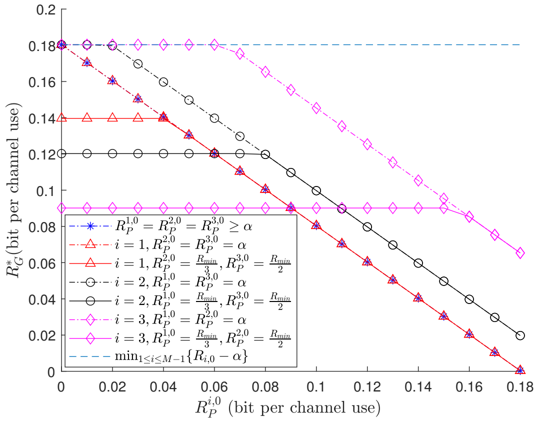


Figure 7. *The relationship between $R_P^{i,0}$ and R_G^* in the star network, where $(\delta_{1,0}^2, \delta_{2,0}^2, \delta_{3,0}^2) = (2.5, 4, 12)$.*

Secondly, $(\delta_{2,0}^2, \delta_{3,0}^2) = (4, 4)$, we consider the two cases for R_G^* in which all segments are consistent (i.e. $R_{1,0}^2 = R_{2,0}^2 = R_{3,0}^2$). The first case is $H(\boldsymbol{K}_{i,0}) = H(\boldsymbol{k}_{i,0}^2), i = 1, 2, 3$ (i.e. $R_P^{1,0} = R_P^{2,0} = R_P^{3,0} = R_{1,0}^2 = R_{2,0}^2 = R_{3,0}^2 = \alpha$). In the second, we set $R_{i,0}^2 = \frac{R_{min}}{2}$ and $H(\boldsymbol{K}_{i,0}) < H(\boldsymbol{k}_{i,0}^2)$ (i.e. $R_P^{1,0} = \frac{R_{min}}{5}, R_P^{2,0} = \frac{R_{min}}{4}, R_P^{3,0} = \frac{R_{min}}{3}$, where $R_{min} = \min_{1 \leq i \leq 3}\{R_{i,0}\}$). From figure 8, when $H(\boldsymbol{K}_{i,0}) = H(\boldsymbol{k}_{i,0}^2)$, the GK rate obtained in our method achieves the upper bound in Eq.(14).

Thirdly, in the mesh network, we set $R_{i,j}^i = R_{i,j}^j, i < j \in \{0, 1, 2, 3\}$, $\beta = 0$ and $R_P^{i,j} = R_{i,j}^{(2)}$. Figure 9a demonstrates the relationship between $\sum_{j=0, j \neq i}^3 R_P^{0,j}$ and R_G^{mesh}. We do not strictly fix $R_P^{i,j}$

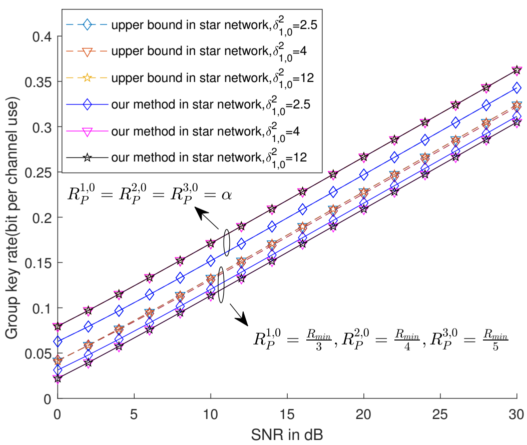
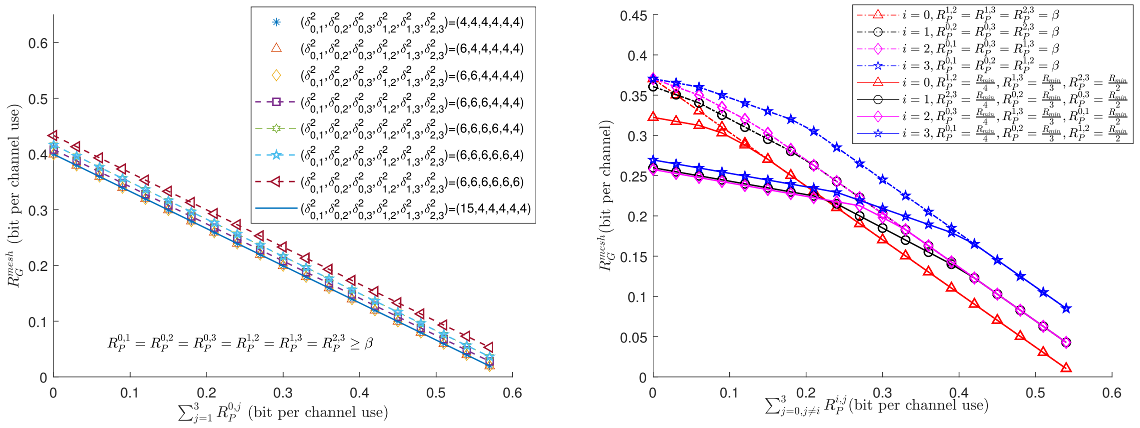


Figure 8. *In the star network, Group Key rate of our scheme (Eq.(11)) and the upper bound (Eq.(14)) in [21], where $(\delta_{2,0}^2, \delta_{3,0}^2) = (4, 4)$.*

(i.e. $R_P^{0,1} = R_P^{0,2} = R_P^{0,3} = R_P^{1,2} = R_P^{1,3} = R_P^{2,3} \geq \beta$). User A_0 has $\sum_{j=1}^3 R_{0,j}$ which is the most in the network (i.e. $\sum_{j=1}^3 R_{0,j} = \max_{0 \leq i \leq 3} \sum_{j=0, j \neq i}^3 R_{i,j}$), we observe that the GK rate increases due to the increase in $min_{0 \leq i \leq 3} \sum_{j=0, j \neq i}^3 R_{i,j}$, but not since $\sum_{j=1}^3 R_{0,j}$.

Furthermore, figure 9b gives the rate relationship between different user A_i's PK and GK, where $(\delta_{0,1}^2, \delta_{0,2}^2, \delta_{0,3}^2, \delta_{1,2}^2, \delta_{1,3}^2, \delta_{2,3}^2) = (2.5, 2.5, 4, 4, 12, 12)$, $R_{min} = \min_{0 \leq i,j \leq 3, j \neq i}\{R_{i,j}\}$. For user A_0, the rate relationship satisfies the triangular region as mentioned in Remark 4 because of $\sum_{j=1}^3 R_{0,j} = R_{min}$. When $\sum_{j=1}^3 R_{0,j} > R_{min}$, the rate relationship is bounded by R_{min}. From figure 9b, it is shown that the relationship for different users satisfies our proposed region in Lemma 4.

Finally, figure 10 represents the GK rate of our scheme compared with the upper bound in Eq.(25) where the values of $\delta_{0,1}^2$ are different. In figure 10a, $R_P^{i,j}$ is expressed as $R_P^{0,1} = R_P^{0,2} = R_P^{0,3} = R_P^{1,2} = R_P^{1,3} = R_P^{2,3} = \beta$. Figure 10b shows that $R_P^{0,1} = R_P^{0,2} = R_P^{0,3} = R_P^{1,2} = R_P^{1,2} = R_P^{2,3} = \frac{R_{min}}{4}$. And in figure 10c, $R_P^{0,1} = \beta, R_P^{0,2} = \frac{R_{min}}{6}, R_P^{0,3} = \frac{R_{min}}{5}, R_P^{1,2} = \frac{R_{min}}{4}, R_P^{1,3} = \frac{R_{min}}{3}, R_P^{2,3} = \frac{R_{min}}{2}$, where $R_{min} = \min_{0 \leq i,j \leq 3, j \neq i}\{R_{i,j}\}$. Therefore, when all $R_P^{i,j}$ are consistent as zero (i.e. $R_P^{0,1} = R_P^{0,2} = R_P^{0,3} = R_P^{1,2} = R_P^{1,3} = R_P^{2,3} = 0$), the GK rate in our method reaches the upper bound only when all channel variances are consistent (i.e. $\delta_{0,1}^2 = \delta_{0,2}^2 = \delta_{0,3}^2 = \delta_{1,2}^2 = \delta_{1,3}^2 = \delta_{2,3}^2 = 4$). When $\delta_{0,1}^2 = 2.5$



(a)

(b)

Figure 9. *The relationship between* $\sum_{j=0,j\neq i}^{3} R_P^{i,j}$ *and* R_G^{mesh} *in the mesh network.*

or 12, there is a gap between our scheme and the upper bound, which is always a constant as the SNR increases. And the value of $R_P^{i,j}$ does not affect the trend of this gap. Thus, we believe that our method in the mesh network achieves the optimal multiplexing gain and PKs do not affect the multiplexing gain of GK, as discussed in Proposition 2.

VI. CONCLUSION

This paper investigated the generation of secret pairwise key (PK) and group key (GK) in dual-task scenarios. Since traditional group key generation methods were subject to inside attack when used directly in this scenario, we proposed segment-based key generation method for generating GK and PK separately. We illustrated the detailed algorithms for star and mesh networks. Our scheme could effectively prevent outside attack and inside attack and had great performance of GK generation. Numerical results indicated that proposed approach could securely fulfill the requirement of dual-task, coinciding with the theoretical analysis.

ACKNOWLEDGEMENT

This work was supported in part by the National Key R&D Program of China(No.2022YFB2902202), in part by the Fundamental Research Funds for the Central Universities(No.2242023K30034), in part by the National Natural Science Foundation of China(No.62171121, U22A2001), in part by the National Natural Science Foundation of Jiangsu Province, China(No.BK20211160), in part by the Southeast University Startup Fund(No.4009012301) and in part by the National Natural Science Foundation of China(No.62301144).

REFERENCES

[1] TANG J, WEN H, SONG H H, et al. Sharing secrets via wireless broadcasting: A new efficient physical layer group secret key generation for multiple iot devices[J]. IEEE Internet of Things Journal, 2022.

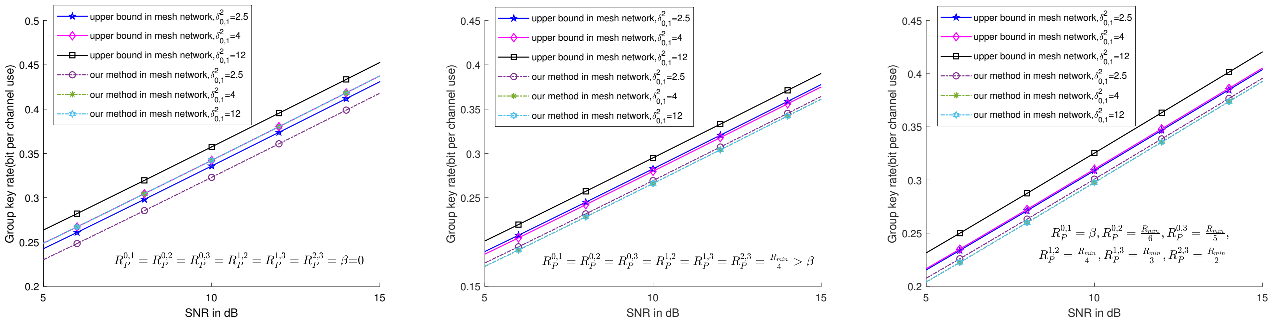
[2] PORAMBAGE P, BRAEKEN A, SCHMITT C, et al. Group key establishment for enabling secure multicast communication in wireless sensor networks deployed for iot applications[J]. IEEE Access, 2015, 3: 1503-1511.

[3] ZHANG J, DUONG T Q, WOODS R, et al. Securing wireless communications of the internet of things from the physical layer, an overview[J]. Entropy, 2017, 19(8): 420.

[4] LI G, ZHANG Z, ZHANG J, et al. Encrypting wireless communications on the fly using one-time pad and key generation[J]. IEEE Internet of Things Journal, 2020, 8(1): 357-369.

[5] CHADHA A. Group key distribution via local collaboration in wireless sensor networks[M]. The University of Texas at Arlington, 2005.

[6] JAIN M K. Wireless sensor networks: Security



(a) **(b)** **(c)**

Figure 10. *In the mesh network, Group Key rate of our scheme (Eq.(22)) and the upper bound (Eq.(25)) in [21], where* $(\delta^2_{0,2}, \delta^2_{0,3}, \delta^2_{1,2}, \delta^2_{1,3}, \delta^2_{2,3}) = (4, 4, 4, 4, 4)$.

issues and challenges[J]. International Journal of Computer and Information Technology, 2011, 2 (1): 62-67.

[7] LI G, HU L, STAAT P, et al. Reconfigurable intelligent surface for physical layer key generation: Constructive or destructive?[J]. IEEE Wireless Communications, 2022.

[8] ZENG K. Physical layer key generation in wireless networks: challenges and opportunities[J]. IEEE Communications Magazine, 2015, 53(6): 33-39.

[9] LINNING P, LI G, ZHANG J, et al. An investigation of using loop-back mechanism for channel reciprocity enhancement in secret key generation [J]. IEEE Transactions on Mobile Computing, 2018, 18(3): 507-519.

[10] LI G, HU A, PENG L, et al. The optimal preprocessing approach for secret key generation from ofdm channel measurements[C]//IEEE Globecom Workshops. 2016: 1-6.

[11] LAI L, LIANG Y, POOR H V. A unified framework for key agreement over wireless fading channels[J]. IEEE Transactions on Information Forensics and Security, 2011, 7(2): 480-490.

[12] NITINAWARAT S, YE C, BARG A, et al. Secret key generation for a pairwise independent network model[J]. IEEE Transactions on Information Theory, 2010, 56(12): 6482-6489.

[13] CHEN C, JENSEN M A. Secret key establishment using temporally and spatially correlated wireless channel coefficients[J]. IEEE Transactions on Mobile Computing, 2010, 10(2): 205-215.

[14] KUMAR M S, RAMANATHAN R, JAYAKUMAR M, et al. Physical layer secret key generation using discrete wavelet packet transform[J]. Ad Hoc Networks, 2021, 118: 102523.

[15] WANG Q, SU H, REN K, et al. Fast and scalable secret key generation exploiting channel phase randomness in wireless networks[C]//IEEE INFOCOM. 2011: 1422-1430.

[16] LIU H, YANG J, WANG Y, et al. Collaborative secret key extraction leveraging received signal strength in mobile wireless networks[C]//IEEE INFOCOM. 2012: 927-935.

[17] THAI C D T, LEE J, PRAKASH J, et al. Secret group-key generation at physical layer for multi-antenna mesh topology[J]. IEEE Transactions on Information Forensics and Security, 2018, 14(1): 18-33.

[18] HARSHAN J, CHANG S Y, HU Y C. Insider-attacks on physical-layer group secret-key generation in wireless networks[C]//IEEE Wireless Communications and Networking Conference. 2017: 1-6.

[19] XU P, CUMANAN K, DING Z, et al. Group secret key generation in wireless networks: algorithms and rate optimization[J]. IEEE Transactions on Information Forensics and Security, 2016, 11(8): 1831-1846.

[20] WEI Y, ZHU C, NI J. Group secret key generation algorithm from wireless signal strength[C]// IEEE Sixth International Conference on Internet Computing for Science and Engineering. 2012: 239-245.

[21] YE C, REZNIK A. Group secret key genera-

tion algorithms[C]//IEEE International Symposium on Information Theory. 2007: 2596-2600.

[22] LI G, HU L, HU A. Lightweight group secret key generation leveraging non-reconciled received signal strength in mobile wireless networks[C]// IEEE International Conference on Communications Workshops (ICC Workshops). 2019: 1-6.

[23] XU P, DING Z, DAI X, et al. Simultaneously generating secret and private keys in a cooperative pairwise-independent network[J]. IEEE Transactions on Information Forensics and Security, 2016, 11(6): 1139-1150.

[24] LIU H, YANG J, WANG Y, et al. Group secret key generation via received signal strength: Protocols, achievable rates, and implementation[J]. IEEE Transactions on Mobile Computing, 2014, 13(12): 2820-2835.

[25] LAI L, LIANG Y, DU W. Cooperative key generation in wireless networks[J]. IEEE Journal on Selected Areas in Communications, 2012, 30(8): 1578-1588.

[26] ZHOU H, HUIE L M, LAI L. Secret key generation in the two-way relay channel with active attackers[J]. IEEE Transactions on Information Forensics and Security, 2014, 9(3): 476-488.

[27] ZHANG J, WOODS R, DUONG T Q, et al. Experimental study on key generation for physical layer security in wireless communications[J]. IEEE Access, 2016, 4: 4464-4477.

[28] LI G, HU A, ZHANG J, et al. High-agreement uncorrelated secret key generation based on principal component analysis preprocessing[J]. IEEE Transactions on Communications, 2018, 66(7): 3022-3034.

[29] LINNING P, LI G, ZHANG J, et al. An investigation of using loop-back mechanism for channel reciprocity enhancement in secret key generation [J]. IEEE Transactions on Mobile Computing, 2018, 18(3): 507-519.

[30] MAURER U M. Secret key agreement by public discussion from common information[J]. IEEE Transactions on Information Theory, 1993, 39 (3): 733-742.

[31] AHLSWEDE R, CSISZR I. Common randomness in information theory and cryptography. i. secret sharing[J]. IEEE Transactions on Information Theory, 1993, 39(4): 1121-1132.

BIOGRAPHIES

Yang Lilin received the B.S. degree in communication engineering from Nanjing Institute of Technology in 2021. She is currently working toward the M.S. degree in Cyber Science and Engineering with Southeast University, Nanjing, China. Her research interests include physical layer security and group key generation. Email: yanglilin@ seu.edu.cn

Li Guyue received the B.S. degree in information science and technology, and the Ph.D. degree in information security from Southeast University, Nanjing, China, in 2011 and 2017, respectively. Her research interests include physical layer security, secret key generation, radio frequency fingerprint, and link signature. Email: guyuelee@seu.edu.cn

Guo Tao received the B.S. degree in Telecommunications Engineering from Xidian University, Xi’an, China, and the Ph.D. degree from the Department of Information Engineering, The Chinese University of Hong Kong, Hong Kong, China, in 2013 and 2018, respectively. His research interests include network information theory, information theory security, privacy protection, and semantic communication. Email: taoguo@seu.edu.cn

Xu Hao received the B.S. degree in communication engineering from the Nanjing University of Science and Technology, Nanjing, China, in 2013, and the Ph.D. degree in information and communication engineering from the National Mobile Communications Research Laboratory, Southeast University, Nanjing, in 2019. His research interests mainly include information theory, mathematical optimization, MIMO systems, D2D communication, and physical layer security in wireless networks. Email: hao.xu@ucl.ac.uk

Hu Aiqun received the B.Sc. (Eng.), M.Eng.Sc., and Ph.D. degrees from Southeast University in 1987, 1990, and 1993, respectively. His research interests include data transmission and secure communication technology. Email: aqhu@seu.edu.cn