## APPENDICES

## APPENDIX A-COMMUNICATION AND COMPUTATION COMPLEXITY

TABLE III: Comparison between PosGKG and related works

| Ref. | | CompC | | CommC-D |
|---|---|---|---|---|
| | | CompC-RFS | CompC-D | |
| [12] | CGKG | $O(NL)$ | $O(L)$ | $\frac{L}{2^l}$ |
| | DGKG | $-$ | $O(N^3L)$ | $(N+1)\cdot\frac{L}{2^l}$ |
| | DHGKG | $O((N^3+N_g)L)$ | $O(N_s^3L)$ | $(N_s+1)\cdot\frac{L}{2^l}$ |
| **PosGKG** | | $-$ | $O(NL)$ | $(N+1)\cdot\frac{L}{2^l}$ |

1. CompC-D: Computation Complexity of a BD; CommC-D: Communication Complexity of BDs (total communication times of BDs in one group).
2. $N$: the number of BDs; $N_s$: the number of BDs in the sub-group; $N_g$: the number of gate-way BDs in the group; $L$: the total length of a group key. $l$: quantization level.
3. Settings: it is noteworthy that the values of CompC and CommC are obtained based on the same number of BDs $N$ in one group.

In this section, we analyze the Communication Complexity (CommC) and Computation Complexity (CompC) of the highly related PHYGKG schemes in comparison with the PosGKG.

As shown in Table III, the CommC and CompC of BDs in CGKG are the lowest compared with DGKG and DHGKG. In CGKG, BDs only need to perform in backscatter mode within a specific time slot and just need to calculate the round-trip channel information based on the round-trip channel information broadcasted by the RFS. Therefore, the CommC and CompC of BDs to generate a group key of length $L$ is $\frac{L}{2^l}$ and $O(NL)$, respectively. Since RFS needs to estimate round-trip channel information and broadcast the round-trip channel difference to the BDs in the group, the CommC of RFS is $O(NL)$ and the CommC of BDs is $O(NL)$. On the other hand, DGKG requires BDs to alternately operate in backscattering mode during designated time slots, maintaining in listening mode during the remaining time slots, and broadcasting the combination of triangle channel information to the other BD. Therefore, in DGKG, the CommC for BDs to generate a group key is $(N+1)\cdot\frac{L}{2^l}$. Since DGKG does not require the RFS to provide additional key generation information, needing only the RFS to operate in broadcast mode. Hence, DGKG does not necessitate extra computations from the RFS. Each BD in the group needs to solve a linear equation via Gauss-Jordan elimination, as detailed in [34], with a computation complexity of $O(N^3)$ for deriving $N(N-1)/2$ pieces of triangle channel information. Hence, the whole GKG process entails a CommC of $O(N^3\cdot\frac{L}{2^l})$. DHGKG integrates the advantages of both the CGKG and DGKG, employing the CGKG to generate the group key among the RFS, and adopting DGKG for the generation of sub-group keys. Hence, the CommC of BDs to generate a group key is $O((N_s^3+1)\cdot\frac{L}{2^l})$, where $N_s$ is the number of BDs in the sub-group. In DHGKG, the RFS utilizes unsupervised classification to divide the group into sub-groups and needs to broadcast the difference round-trip channel information, resulting in a CompC of $O((N^3+N_g)L)$.

Compared to DGKG, PosGKG demonstrates a lower CommC for BDs. As each BD only needs to transform $N$ local coordinates to global coordinates, the CompC for extracting SI is $O(N)$. Hence, the CompC of PosGKG to generate a group key of length $L$ is $O(NL)$, which is significantly lower than that of DGKG. Similar to DGKG, PosGKG requires BDs to alternately operate in backscattering mode during designated time slots, maintain listening mode during the remaining time slots, and broadcasting the distance information between itself and RFS to the other BDs. Hence, the CommC of PosGKG is also $(N+1)\cdot\frac{L}{2^l}$.

## APPENDIX A-SECURITY ANALYSIS

In this section, we examine the secret key rate that can be achieved by PosGKG in the presence of an eavesdropper, a process analogous to that described in reference [12]. Within the PosGKG framework, each BD must broadcast the distance between the RFS and itself. Compared to passive attacks, active attacks lead to an increase in the shared key information and the attackers control additional information. As long as the consistency of the SI is not compromised, the secure achievable key rate during passive attacks can be easily used to derive the achievable secure key rates for various active attacks. Due to space limitations, this paper only presents the secure achievable key rate of PosGKG under passive attacks. Consequently, the downlink channel distance matrix, denoted as $D_d$, is known to all parties in the public domain. The common information, or shared randomness, among the group is represented by the set $P_G = \{GC_1, GC_2, \ldots, GC_N\}$. This scenario can be considered a specific instance of Slepian-Wolf coding, as discussed in [35]. Therefore, we define the lossless coding rates accordingly.

$$Rate_{Key}(M) = \frac{1}{M}H(GC_1(M), GC_2(M), ..., GC_N(M)), \tag{11}$$

where $H(\cdot)$ denotes the entropy calculation of a given sequence, where $(i)$ indicates the $i^{th}$ round of key generation. $P_G(i)$ represents the set of global coordinates at the $i^{th}$ key generation event, and $GC_i(M) = \{GC_i(1), GC_i(2), ..., GC_i(M)\}$ denotes the set of measurements for the $i^{th}$ round. We define $Rate_{Pro}$ as the rate of information that the RFS must supply to the BDs within the group exhibiting the 'worst' observation for the purpose of generating the group key, as referenced in [35]. The expression for $Rate_{pro}$ is given as follows:

$$Rate_{Pro}(M) = \max_{1\le i\le N}\frac{1}{M}I([GC_1(M), ..., GC_N(M)]|D_d(M), GC_i(M)), \tag{12}$$

where $D_d(M) = [d_1(M), d_2(M), ..., d_N(M)]$. With the Slepian-Wolf source encoding with the above random binning structure, the key mismatch probability goes to 0 as $M\to\infty$ and the upper bound of key rate can be obtained. With the above analysis, we can now define the asymptotic group information rate [35]:

$$\begin{aligned} Rate_{Asym}(M) &= \lim_{M\to\infty} Rate_{Key}(M) - Rate_{Pro}(M) \\ &= \min_{1\le i\le N}\lim_{M\to\infty}\frac{1}{M}I([GC_1(M), ..., GC_N(M)]; [D_d(M), GC_i(M)]). \end{aligned} \tag{13}$$

Since the downlink channel distance matrix $D_d$ is known in the public, which helps an eavesdropper (Eve) to construct the local coordinate set $P_L^e = [L_1^e, L_2^e, \ldots, L_N^e]$. It's noteworthy that since Eve does not possess a private weight vector $w$, Eve can not convert the local coordinate set to the global coordinate set. Therefore, the key compromised by Eve can be expressed as $V_e(M) = \{P_L^e(1), ..., P_L^e(M)\}$. And we define the key rate between the common information of the BD group and the eavesdropped information by Eve as:

$$Rate_{Eve}(M) = \lim_{M\to\infty}\frac{1}{M}I([GC_1(M), ..., GC_N(M)]; [D_d(M), V_e(M)]). \tag{14}$$

Now, we can write the achievable Secret Key Rate (SKR) as:

$$Rate_{Sec}(M) = Rate_{Asym}(M) - Rate_{Eve}(M). \tag{15}$$

Since the observation of each BD is identically distributed, $Rate_{Sec}$ can be obtained by analyzing the SKR for an arbitrary BD (say $A_i$).

The SKR of PosGKG given in equation (15) can be written after dropping key length indices for simplicity as follows:

$$\begin{aligned} Rate_{Sec} &= I([GC_1, ..., GC_N]; [D_d, GC_i]) - I([GC_1, ..., GC_N]; [D_d, V_e]) \\ &= I([GC_1, ..., GC_N]; GC_i | D_d) - I([GC_1, ..., GC_N]; V_e | D_d). \end{aligned} \tag{16}$$

We can use the chaining rule of mutual information to perform the following transformations to $I([GC_1, ..., GC_N]; GC_i|D_d)$ and $I([GC_1, ..., GC_N]; V_e|D_d)$:

$$\begin{aligned} Rate_{GenLower} &= I(\boldsymbol{GC}; GC_i|D_d) = I([GC_1, ..., GC_N]; GC_i|D_d) \\ &= I(GC_j; GC_i|D_d) + I([GC_1, ..., GC_{j-1}, GC_{j+1} \\ &, ..., GC_N]; GC_i|GC_j, D_d) \geq I(GC_j; GC_i|D_d). \end{aligned} \tag{17a}$$

$$\begin{aligned} Rate_{EveUpper} &= I\left(\boldsymbol{GC}; V_e \mid D_d\right) = I\left(\boldsymbol{GC}; Cor\boldsymbol{GC}^T \mid D_d\right) \\ &= I\left([GC_1, \ldots, GC_N]; [cor_1 GC_1, ..., cor_N GC_N] \mid D_d\right) \\ &= \sum_{j=1}^{N} I\left(GC_j; V_e \mid [GC_1, \ldots, GC_{j-1}], D_d\right) \leq H(V_e, D_d) \\ &= H([cor_1 GC_1, ..., cor_N GC_N], D_d) = H(Cor\boldsymbol{GC}^T, D_d) \end{aligned} \tag{17b}$$

where $cor_i$ represents the cross-correlation between the global coordinates obtained by the legitimate device and the eavesdropper. Therefore, the lower-bound of Key Generation Rate (KGR) and SKR is $Rate_{GenLower} = I(GC_j; GC_i|D_d)$ and $Rate_{GenLower} - Rate_{EveUpper} = I(GC_j; GC_i|D_d) - H(Cor\boldsymbol{GC}^T, D_d)$ , respectively. As the attacker cannot obtain the private weight vector that is correlated to legitimate BDs, that is $W_i \perp W_e$, then for any $cor_i$ in $Cor$ has $cor_i \approx 0$. That is $Cor\boldsymbol{GC}^T \perp D_d$ and $H(Cor\boldsymbol{GC}^T, D_d) \approx 0$. $\perp$ represents two variables are uncorrelated or independent. Consequently, the upper bound of the eavesdropping rate approaches zero since the eavesdropper is unable to acquire a private weight vector that is correlated with the legitimate BDs. **We can conclude that PosGKG has strong robustness in the presence of eavesdropper.**