## APPENDICES

### 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 [41]. Therefore, we define the lossless coding rates accordingly.

$$\begin{aligned} Rate_{Key}(M) &= \frac{1}{M} H(P_G(1), P_G(2), ..., P_G(M)) \\ &= \frac{1}{M} H(GC_1(M), GC_2(M), ..., GC_N(M)), \end{aligned} \tag{13}$$

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 [41]. The expression for $Rate_{pro}$ is given as follows:

$$Rate_{Pro}(M) = \max_{1 \le i \le N} \frac{1}{M} I([GC_1(M), ..., GC_N(M)] | D_d(M), GC_i(M)), \tag{14}$$

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 the key rate can be obtained. With the above analysis, we can now define the asymptotic group information rate [41]:

$$\begin{aligned} Rate_{Asym}(M) &= \lim_{M \to \infty} Rate_{Key}(M) - Rate_{Pro}(M) \\ &= \min_{1 \le i \le N} \lim_{M \to \infty} \frac{1}{M} I([GC_1(M), ..., GC_N(M)]; [D_d(M), GC_i(M)]). \end{aligned} \tag{15}$$

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 cannot 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:

$$Rate_{Eve}(M) = \lim_{M \to \infty} \frac{1}{M} I([GC_1(M), ..., GC_N(M)]; [D_d(M), V_e(M)]). \tag{16}$$

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

$$Rate_{Sec}(M) = Rate_{Asym}(M) - Rate_{Eve}(M). \tag{17}$$

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 (17) can be written after dropping key length indices for simplicity as follows:

$$\begin{aligned} Rate_{Sec} &= I([GC_1, ..., GC_N]; [D_d, GC_i]) - I([GC_1, ..., GC_N]; [D_d, V_e]) \\ &= I([GC_1, ..., GC_N]; GC_i | D_d) + I([GC_1, ..., GC_N]; D_d) \\ &\quad - I([GC_1, ..., GC_N]; V_e | D_d) - I([GC_1, ..., GC_N]; D_d) \\ &= I([GC_1, ..., GC_N]; GC_i | D_d) - I([GC_1, ..., GC_N]; V_e | D_d). \end{aligned} \tag{18}$$

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 $I([GC_1, ..., GC_N]; V_e | D_d)$:

$$\begin{aligned} Rate_{GenLower} &= I(\boldsymbol{GC}; GC_i | D_d) = I([GC_1, ..., GC_N]; GC_i | D_d) \\ &= I(GC_j; GC_i | D_d) + I([GC_1, ..., GC_{j-1}, GC_{j+1} \\ &\quad , ..., GC_N]; GC_i | GC_j, D_d) \ge I(GC_j; GC_i | D_d). \end{aligned} \tag{19a}$$

$$\begin{aligned} Rate_{EveUpper} &= I(\boldsymbol{GC}; V_e \mid D_d) = I\left(\boldsymbol{GC}; Cor\boldsymbol{GC}^T \mid D_d\right) \\ &= I\left([GC_1, \ldots, GC_N]; [cor_1 GC_1, ..., cor_N GC_N] \mid D_d\right) \\ &= \sum_{j=1}^{N} I\left(GC_j; V_e \mid [GC_1, \ldots, GC_{j-1}], D_d\right) \le H(V_e, D_d) \\ &= H([cor_1 GC_1, ..., cor_N GC_N], D_d) = H(Cor\boldsymbol{GC}^T, D_d) \end{aligned} \tag{19b}$$

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.**

### APPENDIX B-METHODS FOR MITIGATING SMA

The primary interference mechanism of SMA attacks on PosGKG manifests as the disruption of measurement consistency in RSS and AoA among legitimate devices, consequently leading to mismatched positional information between devices. Therefore, the core of effective SMA defense lies in accurately distinguishing the RSS and AoA measurement results between legitimate devices and attackers.

OFDMA technology achieves RSS separation between attack signals and legitimate device signals through frequency-domain isolation. The key characteristics of this technology

include: 1) dividing the total frequency band into multiple orthogonal subcarriers, and 2) allocating mutually exclusive subcarrier groups (sub-channels) to different devices. Leveraging the orthogonality between subcarriers, signals from various devices can achieve interference-free superposition in the frequency domain [19]. During signal transmission, legitimate devices utilize pre-allocated subcarrier groups, while attackers randomly occupying frequency bands struggle to maintain orthogonality with legitimate subcarriers. This non-orthogonality induces Inter-Carrier Interference (ICI), causing degradation in the attack signal's own quality while having minimal impact on legitimate subcarrier transmission. Furthermore, even when attackers target idle subcarriers, the spatial channel differences between attackers and legitimate devices can still provide an auxiliary discriminative basis for precise RSS separation.

To achieve effective AoA separation between legitimate device signals and attack signals, a redundant antenna design approach must be employed. While OFDMA technology resolves frequency-domain interference through orthogonal subcarrier allocation, it cannot enhance the spatial resolution capability of antennas. Consequently, antenna redundancy design is essential to ensure sufficient spatial degrees of freedom. Specifically, when the number of legitimate devices operating in backscatter mode within a single time slot is $N_b$ and the number of SMA attackers is $N_{SMA}$, the constraint $N_{an} \geq N_b + N_{SMA} + 1$ must be perpetually satisfied. Given that $N_{an}$ remains fixed while $N_{SMA}$ varies dynamically, the system can maintain this inequality through real-time adjustment of $N_b$.For real-time estimation of $N_{SMA}$, the following indicators should be monitored: 1) Abnormal increase in unauthorized subcarrier count 2) Deviations of RSS or CIR from whitelist thresholds. When $N_{an} < N_b + N_{SMA} + 1$ is detected, the RFS should immediately terminate the key generation process and reduce the number of active legitimate devices per time slot to $N_b'$ to re-establish compliance with the constraint. The detailed implementation of this dynamic adjustment mechanism will be addressed in subsequent research.