# 論文内容の要旨

申請者氏名　　QU QIANYUE

Millimeter wave (mmWave) communication has emerged as a promising technology for next-generation wireless networks due to its abundant spectrum resources and potential for multi-gigabit-per-second data rates. However, the inherent broadcast nature of wireless transmissions and unique characteristics of mmWave propagation introduce new security vulnerabilities, particularly to eavesdropping attacks. Physical layer security (PLS), which exploits the inherent characteristics of wireless channels to ensure secure communication, offers a promising complementary approach to traditional cryptographic methods.

This thesis investigates PLS mechanisms in two critical mmWave wireless communication scenarios. First, we study the eavesdropping behavior in hybrid communication systems where mmWave and microwave links coexist, which is the ground-to-ground (G2G) scenario. We propose a novel analytical framework to characterize eavesdropping regions based on the eavesdropper's selection behavior between mmWave and microwave transmissions. Through comprehensive analysis of secrecy outage probability (SOP) and secrecy rate metrics, we reveal how system parameters such as blockage density and selection preferences influence the eavesdropping regions. We further establish an optimization framework to determine optimal eavesdropping locations, demonstrating through numerical results that the eavesdropping region significantly decreases with increasing blockage density and varies with the eavesdropper's selection parameter.

Second, we explore secure transmission in Unmanned Aerial Vehicle (UAV)-enabled mmWave multicast systems, which is the air-to-ground (A2G) scenario. A UAV serves as an aerial base station to transmit confidential information to multiple ground users in the presence of eavesdroppers. We develop a comprehensive optimization framework that jointly considers UAV deployment and resource allocation to enhance physical layer security. Our analysis reveals the fundamental trade-off between security and coverage, showing that user group distribution characteristics significantly impact the optimal UAV altitude and achievable secrecy rates. Through extensive theoretical analysis and numerical simulations, we demonstrate that well-clustered user groups achieve superior secrecy performance at lower UAV altitudes, while dispersed groups require higher altitudes at the cost of reduced secrecy rates. The proposed optimization approaches provide practical guidelines for implementing secure UAV-aided mmWave communications while maintaining quality of service requirements.

# 論文審査結果の要旨

申請者氏名　　QU QIANYUE

令和6年12月24日に開催した公聴会の結果を参考に令和7年2月10日に博士論文の審査を行った．以下の通り，本博士論文は，提案者が独立した研究者として研究活動を続けていくための十分な素養を備えていることを示すものと認める．

Qu Qianyue氏は，本博士論文において，次世代無線ネットワークの基盤技術として注目されているミリ波通信に対し，地上間と空対地の二種類の通信環境における物理層セキュリティ技術の適用性評価に向けた理論的フレームワークの検討を行なっている．本論文の貢献は以下のようにまとめることができる．

1. ミリ波とマイクロ波が共存する地上間通信環境における盗聴状況に着目し，システム・アンテナ・遮蔽・伝搬のそれぞれの部分モデルから統合モデルを構成し，ミリ波通信とマイクロ波通信の両方における秘密保持劣化率 (Secrecy Outage Probability: SOP) と秘匿レート (Secrecy Rate) を理論的に導出するフレームワークを確立した．

2. ミリ波とマイクロ波が共存した地上間通信環境におけるセキュリティ評価指標の秘密保持劣化率と秘匿レートについて，障害物密度や盗聴者の通信チャネル選択パラメータを変化させたときの評価指標の変化を計算機シミュレーションによって定量的に精査し，障害物密度が増加するにつれて盗聴領域が大幅に縮小すること，盗聴者の選択パラメータが盗聴可能範囲に大きく影響を与えること，といった特性を明らかにした．

3. ミリ波を活用して無人航空機 (Unmanned Aerial Vehicle: UAV) が複数の地上局とマルチキャスト通信を行う環境に着目し，高い秘匿性を保証するように空中基地局UAVの配置とミリ波マルチキャスト通信における送信電力の同時最適化を行うフレームワークを確立した．

4. UAVによる空対地のマルチキャスト通信の最適化フレームワークを基に計算機シミュレーションを行い，セキュリティとマルチキャスト通信のカバレッジの間にトレードオフが存在すること，地上ユーザの分布特性が最適なUAV高度や秘匿レートに大きな影響を与えることを明らかにした．

提案された二つのフレームワークはいずれもミリ波通信の特徴を高度に捉えた盗聴可能領域同定アプローチを提供しており，秘密保持劣化率や秘匿レートの数値例を通して得られたセキュリティと環境パラメータとの関係性はミリ波通信に物理層セキュリティ技術を適用していく上で基礎的な知見を与える点で有用性が高く，情報通信工学の貢献に加えて実学的観点からも高い意義が認められる．

よって，本論文は，博士（工学）の学位論文として価値あるものと認める．