URSI AP-RASC, Sydney, Australia, 17 – 22 August 2025

Secrecy Performance Analysis with Air-to-Ground Regime over Nakagami-*m* Fading Channels Based on Statistical Models

Huan Huang [(1)], Lixin Guo * [(1)], and Zhongyu Liu[(1)]
(1) Xidian University, Shannxi, China; e-mail: 23201110153@stu.xidian.edu.cn; lxguo@xidian.edu.cn; liuzy@xidian.edu.cn

Abstract

Based on the 3rd Generation Partnership Project (3GPP) urban microcell air-to-ground (A2G) path loss statistical model, the secrecy performance of communication systems in realistic urban environments under Nakagami-*m* fading channels is investigated in this paper. We systematically compare the path loss coverage and secrecy outage probability (SOP) coverage of unmanned aerial vehicle (UAV)-enabled aerial base stations at different altitudes. Furthermore, a receiver location selection scheme that leverages path loss prediction results from signal transmitters is proposed to optimize legitimate receiver positioning, thereby enhancing overall secrecy performance. The analytical framework provides new insights into the altitude-dependent tradeoffs between coverage reliability and physical-layer security in UAV-assisted cellular networks.

1. Introduction

Benefiting from remarkable advancements in payload capacity and battery endurance, UAVs have witnessed rapidly expanding applications from conventional military surveillance to diversified civil missions including remote sensing and emergency rescue. Recently, to address the ever-increasing demands for ultra-reliable low-latency communications, UAV-assisted communication architectures equipped with low-cost transceivers academia was proposed [1]. These architectures enable seamless integration with existing cellular networks by deploying UAVs as low-altitude aerial base stations (ABSs) [2]. However, the open nature of wireless channels makes UAV communications more vulnerable to eavesdropping attacks, while the inherent computational constraints of UAVs hinder the implementation of sophisticated encryption schemes. To resolve this contradiction, physical layer security (PLS) techniques exploiting inherent wireless channel characteristics have emerged as a viable solution.

The theoretical foundation of information-theoretic security was established by Wyner's seminal work [3], which introduced the wiretap channel model and characterized the achievable secrecy capacity region. Subsequent contributions from Cheong, Hellman, and Bloch systematically advanced this field, promoting PLS applications in various scenarios [4, 5]. For A2G channels, existing studies have achieved notable progress: a closed-form secrecy outage probability expression for UAV relay systems under Nakagami-m fading is derived in [6], [7] developed a joint pilot optimization and secure transmission framework for UAV base stations; analytical secrecy outage models for randomly moving UAVs were established in [8], [9] investigated security threats posed by UAV eavesdroppers. Nevertheless, current research predominantly neglects realistic urban environment modeling, which motivates our investigation.

This paper innovatively establishes an analytical framework for A2G channel security performance in urban environments, with three key contributions: (1) A 3D spatial discretization model is built based on 3GPP standards, characterizing regional propagation properties through path loss computations at sub-region centroids; (2) A composite channel model is constructed incorporating both path loss and Nakagami-m fading to capture receiver randomness; (3) Secrecy Performance Analysis and Transmitter Positioning Optimization Design Based on Channel Reciprocity in A2G Channels are proposed.

2. System Model and Path Loss Model

Consider an UAV-assisted air-to-ground communication system consisting of a transmitter (Alice), a legitimate receiver (Bob), and an eavesdropper (Eve), each equipment is equipped with a single omnidirectional antenna. In this system model, Alice is deployed as an aerial platform to perform wireless transmission tasks. We assume that the signal amplitude fading characteristics at both Bob and Eve receivers follow the Nakagami-*m* distribution, the background noise is modeled as additive white Gaussian noise (AWGN) characterized by a zero mean and a variance of N_0 , so, the Signal-to-Noise Ratio (SNR) of γ_i for $i \in \{b,e\}$ is given by [10] :

$$f_{\gamma_i}(x) = \left(\frac{m}{\Omega_i}\right)^m \frac{x^{m-1}}{\Gamma(m)} \exp\left(-\frac{m}{\Omega_i}x\right) \quad (1),$$

and the SOP can be written as [10], where R_{th} is the predefined threshold of secrecy capacity (SC), m_{B} and m_{E} are the shape parameter of Nakagami-*m* distribution for Bob and Eve. ω_{B} and ω_{E} are the SNR of Bob and Eve.

$$P_{\mathrm{out}}^{(1)}(R_{\mathrm{th}}) = 1 - \exp\left(\frac{-m_{\mathrm{B}}}{\omega_{\mathrm{B}}}[2^{R_{\mathrm{th}}}-1]\right) \times \sum_{k=0}^{m_{\mathrm{B}}-1}\left(\frac{\omega_{\mathrm{B}}}{m_{\mathrm{B}}}\right)^{k+1-m_{\mathrm{B}}} \times 2^{R_{\mathrm{th}}(m_{\mathrm{B}}-1-k)} \sum_{n=0}^{m_{\mathrm{B}}-1-k}\binom{n+m_{\mathrm{E}}-1}{n}\left(\frac{m_{\mathrm{E}}}{\omega_{\mathrm{E}}}\right)^{-n} \times \frac{\left[1-2^{-R_{\mathrm{th}}}\right]^{m_{\mathrm{B}}-k-n-1}}{(m_{\mathrm{B}}-k-n-1)!\left[1+\frac{\omega_{\mathrm{E}}}{\omega_{\mathrm{B}}}2^{R_{\mathrm{th}}}\right]^{n+m_{\mathrm{E}}}}, \quad (2).$$

Regarding path loss modeling, the urban microcell A2G path loss model specified in the 3GPP TR 36.777 standard is adopted [11], with its mathematical expression formulated as follows:

$$PL' = 32.44 + 20\log_{10}\left(\frac{d_{3\mathrm{D}}}{1\mathrm{km}}\right) + 20\log_{10}\left(\frac{f_c}{\mathrm{MHz}}\right) \quad (3),$$

$$PL_{UMi-AV-LOS} = \max\left\{PL',\ 30.9 + \left(22.25 - 0.5\log_{10}(h_{\mathrm{UT}})\right)\log_{10}(d_{3\mathrm{D}}) + 20\log_{10}(f_c)\right\} \quad (4),$$

$$PL_{UMi-AV-NLOS} = \max\left\{PL_{UMi-AV-LOS},\ 32.4 + \left(43.2 - 7.6\log_{10}(h_{\mathrm{UT}})\right)\log_{10}(d_{3\mathrm{D}}) + 20\log_{10}(f_c)\right\} \quad (5),$$

where PL' represents the free space path loss, $d_{3\mathrm{D}}$ is the 3D distance between the transmitting and receiving antennas in meters, f_c is the frequency of the transmitted signal in gigahertz, h_{UT} is the height of the receiving antenna in meters.

3. Prediction of Received Signal Power

The simulation environment is configured with the Xidian University and its adjacent regions. The corresponding building geometric modeling data is presented in Figure 1.

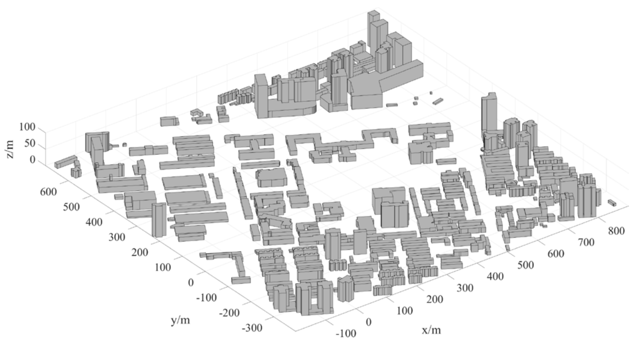

Figure 1. The schematic diagram of building modeling for Xidian University and its surrounding areas.

The TX's height is set to 150 m (above ground level) for enhanced diffraction-dominated coverage, while the RX height is configured at 2 m to emulate typical mobile terminal operation. The transmit signal power is set to 30 dBm. The corresponding received power coverage is subsequently computed and visualized in Figure 2 and Figure 3.

As observed from the comparative analysis in Figures 2 and 3, the elevation of UAV platform altitude induces a gradual transition from non-line-of-sight (NLoS) to line-of-sight (LoS) propagation paths. This propagation characteristic transformation manifests two distinct physical-layer effects: the received power for originally NLoS-conditioned nodes experiences a significant improvement with altitude increase, while the existing LoS links exhibit a gradual degradation in received power due to the amplified path loss caused by higher operational altitude.

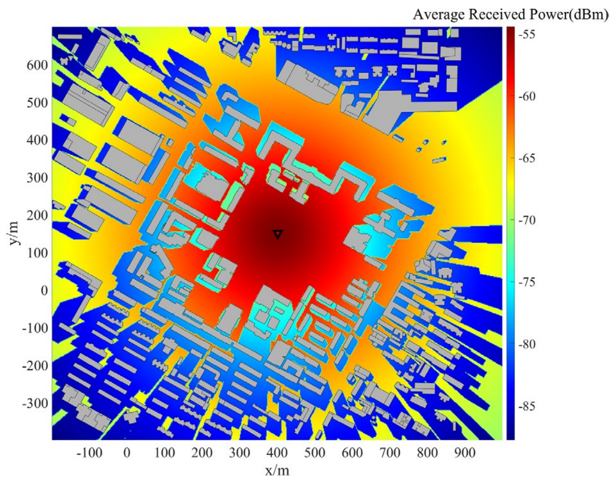

Figure 2. Received power coverage, where transmitting antenna is located at red inverted triangle and the height of TX is 150m.

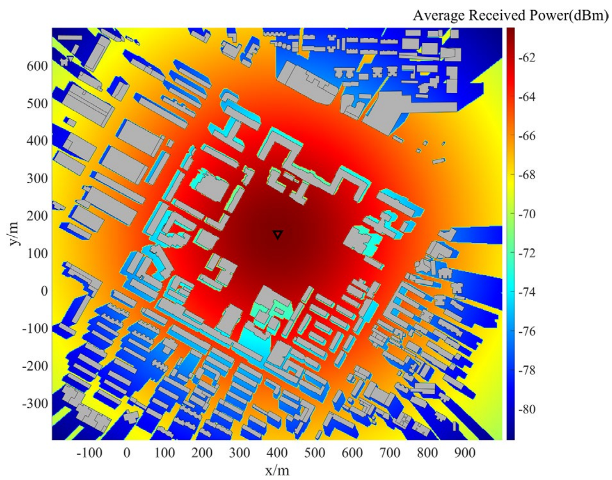

Figure 3. Received power coverage, where transmitting antenna is located at red inverted triangle and the height of TX is 300m.

4. Analysis of Secrecy Performance

Consider a scenario with background noise $N_0 = -90$ dBm, where the Nakagami-m fading parameters for LOS and NLOS channels are configured as $m_{LOS} = 3$ and $m_{NLOS} = 1$, the predefined threshold R_{th} is set to 1. respectively. Assuming Eve is uniformly distributed over the spatial domain, the SOP coverage is illustrated in the Figure 4.

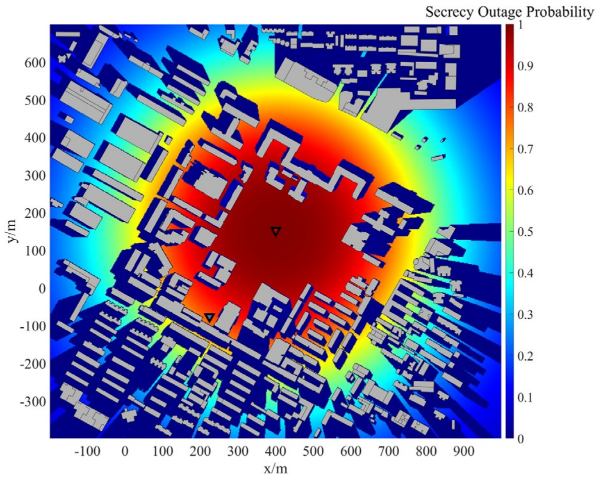

Figure 4. SOP coverage when $N_0 = -90$ dBm, $m_{LOS} = 3$, $m_{NLOS} = 1$, and $R_{th} = 1$. where transmitting antenna is located at red inverted triangle and the height of TX is 300m, and Bob is located at blue inverted triangle and the height is 2m.

As illustrated in Figure 4, the Alice's LOS propagation environment enables distant locations to receive strong signal coverage. To mitigate this coverage imbalance, we strategically relocated Alice's position to the lower-left building cluster while maintaining Bob's original coordinates. The corresponding average received power coverage under new location of Alice is presented in Figure 5.

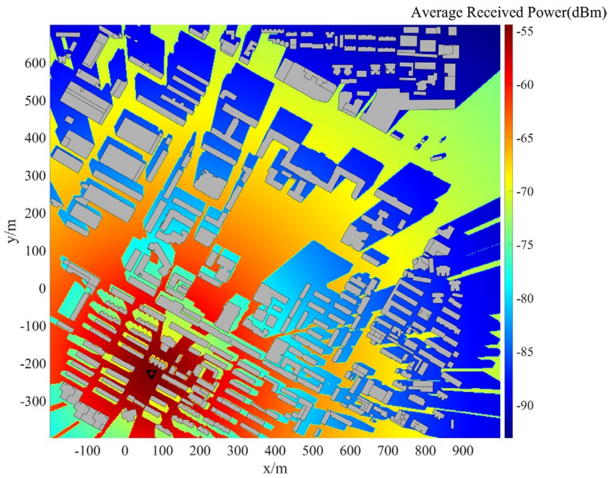

Figure 5. Received power coverage, where transmitting antenna is located at red inverted triangle and the height of TX is 150m.

The corresponding SOP coverage under this optimized configuration is presented in Figure 6, demonstrating significant improvement in physical layer security metrics compared to the baseline scenario.

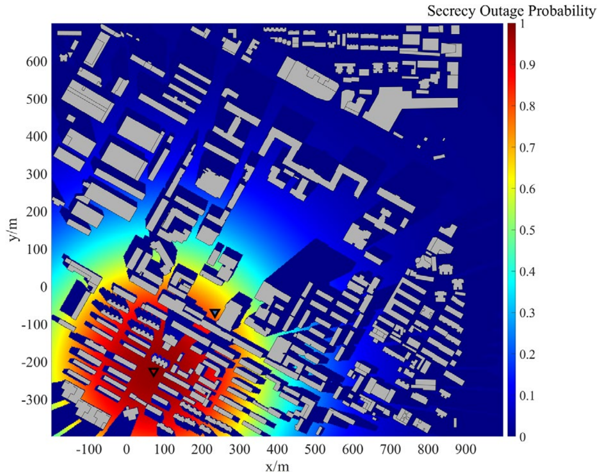

Figure 6. SOP coverage when $N_0 = -90$ dBm, $m_{LOS} = 3$, $m_{NLOS} = 1$, and $R_{th} = 1$. where transmitting antenna is located at red inverted triangle and the height of TX is 300m, and Bob is located at blue inverted triangle and the height is 2m.

On the other hand, when the locations of Alice and Eve are known, the deployment location of Bob can be more freely selected based on Alice's signal coverage characteristics. Taking Figure 5 as an example, when Eve's position fixed, the secrecy outage probability corresponding to each possible location of Bob is calculated and presented in Figure 7.

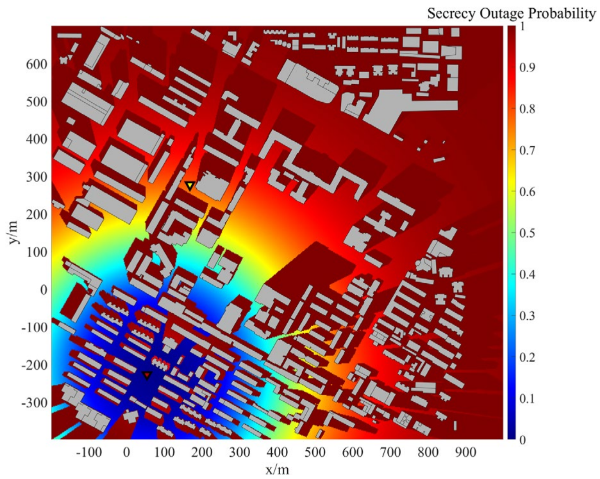

Figure 7. SOP coverage when $N_0 = -90$ dBm, $m_{LOS} = 3$, $m_{NLOS} = 1$, and $R_{th} = 1$. where transmitting antenna is located at red inverted triangle and the height of TX is 300m, and Eve is located at blue inverted triangle and the height is 2m.

5. Conclusion

In this work, a secrecy performance analysis method for A2G communication systems in deterministic urban environments is investigated, leveraging the 3GPP path loss statistical models. The SOP of Eve at different locations is analytically derived when Alice operates as an aerial base station. Furthermore, the impact of Alice's deployment positions on the overall secrecy performance is systematically examined. Notably, when Eve's location is a priori known, we demonstrated that Bob's position can be optimally selected based on Alice's received power coverage to enhance secrecy performance. This study is expected to provide valuable insights for implementing physical-layer security in practical urban secure communication scenarios.

6. Acknowledgements

This work was supported in part by the National Key Laboratory Fund of Electromagnetic Environment (Grant No. JCKY2024210C61424030301), the key project of Social Governance and Scientific and Technological Support for Smart Society (Grant No. 2022YFC3301403), and the Foundation of China Information Technology Designing & Consulting Institute Co. Ltd..

References

[1] A. Fotouhi et al., “Survey on UAV cellular communications: Practical aspects, standardization advancements, regulation, and security challenges,” *IEEE Communications Surveys & Tutorials*, **21**, 4, October 2019, pp. 3417-3442, doi: 10.1109/COMST.2019.2906228.

[2] X. Wang, H. Zhang, Y. Tian, and V. C. M. Leung, “Modeling and analysis of aerial base station-assisted cellular networks in finite areas under LoS and NLoS propagation,” *IEEE Transactions on Wireless Communications*, **17**, 10, October 2018, pp. 6985–7000, doi: 10.1109/TWC.2018.2865344.

[3] A. D. Wyner, “The wire-tap channel,” *Bell System Technical Journal*, 54, 8, 1975, October, pp. 1355–1387, doi: 10.1002/j.1538-7305.1975.tb02040.x.

[4] S. L.-Y. Cheong and M. Hellman, “The Gaussian wire-tap channel,” *IEEE Transactions on Information Theory*, **24**, 4, July 1978, pp. 451–456, doi: 10.1109/TIT.1978.1055917.

[5] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, “Wireless information-theoretic security,” *IEEE Transactions on Information Theory*, **54**, 6, June 2008, pp. 2515–2534, doi: 10.1109/TIT.2008.921908.

[6] L. Kong, Y. Zou and B. Li, "Security and Reliability Tradeoff of UAV Relays Assisted Cognitive Transmissions With Hardware Impairments," *IEEE Internet of Things Journal*, **11**, 6, March 2024, pp. 10336-10351, doi: 10.1109/JIOT.2023.3327577.

[7] Y. Chen, X. Zhang, F. Yao, K. An, G. Zheng and S. Chatzinotas, "Pilot Assignment and Power Control in Secure UAV-Enabled Cell-Free Massive MIMO Networks," *IEEE Internet of Things Journal*, **11**, 2, January 2024, pp. 3377-3391, doi: 10.1109/JIOT.2023.3296736.

[8] X. Yuan, Z. Feng, W. Ni, Z. Wei, R. P. Liu and J. A. Zhang, "Secrecy Rate Analysis Against Aerial Eavesdropper," *IEEE Transactions on Communications*, **67**, 10, October 2019, pp. 7027-7042, doi: 10.1109/TCOMM.2019.2927449.

[9] X. Yuan, Z. Feng, W. Ni, R. P. Liu, J. A. Zhang and W. Xu, "Secrecy Performance of Terrestrial Radio Links Under Collaborative Aerial Eavesdropping," *IEEE Transactions on Information Forensics and Security*, **15**, 2020, pp. 604-619, doi: 10.1109/TIFS.2019.2922353.

[10] A. Omri and M. O. Hasna, “Average secrecy outage rate and average secrecy outage duration of wireless communication systems with diversity over nakagami-m fading channels,” *IEEE Transactions on Communications*, 17, 6, 2018, June, pp. 3822–3833, doi: 10.1109/TWC.2018.2816648.

[11] 3GPP, “Study on Enhanced LTE Support for Aerial Vehicles (release 15),” V1.0.0, 2017.