Novel Nakagami-*m* Channel Model for G2A UAV Communications and Improved Security in Eavesdropping Dense Urban Environments

Evangelos Xenos, Sarmad Ozan, Shuping Dang, Simon Armour, Andrew Austin, and Mark A. Beach
Communication Systems and Networks Research Group, University of Bristol, Bristol, United Kingdom
Email: {evangelos.xenos, s.ozan, shuping.dang, simon.armour, a.austin, m.a.beach}@bristol.ac.uk

***Abstract*—This work achieves improvement in secrecy capacity of values over 50 Mbit/s in the presence of a friendly airborne UAV where previously C_s was less than 10Mbit/s. In addition to the C_s estimation, a study on improving the outage probability of the network was also conducted showing that 10 times lower outages are achieved where previously 60% of the time the system was suffering from such outages. Finally, a closed-form solution is also presented for a Nakagami-m fading channel derived by the properties of a physical system based on the latest 3GPP standard, using a simulation setup for a dense urban environment using a 20MHz bandwidth signal with a center frequency of 2.4GHz with devices distanced from 50 to 650 m, aided by a UAV and in the presence of a UAV eavesdropper.**

***Index Terms*—UAV, eavesdropping, dense urban environment, Nakagami, secrecy capacity, outage probability, channel model**

I. Introduction

Metropolitan cities worldwide often suffer from insufficient resources available within existing networks to sufficiently cover and support high bandwidth reliable communication. Unmanned Aerial Vehicles (UAVs) have become a very popular solution to establish reliable communication links in the most extreme locations or where additional infrastructure is financially not viable to be installed. However, UAV-aided communications can suffer from eavesdropping and malicious attacks to intercept data and compromise communications security [1] [2]. Unmanned aerial vehicles (UAVs) have become increasingly prominent for their versatility, cost-effectiveness, and unmatched automation capabilities [3], [4]. Thanks to the remarkable strides made in drone technology, tasks that were once deemed impossible or prohibitively expensive can now be undertaken. UAVs have proven invaluable across various sectors, such as civilian, research, or military purposes. They provide enhanced mobility, network coverage, and critical infrastructure support, making them indispensable tools in numerous domains. As UAV technology advances, their applications and benefits are expected to soar, further augmenting their usefulness in modern society. One particularly exciting development in UAV technology is their ability to enhance network coverage in urban areas and eliminate signal blind spots. The towering steel and concrete structures of big cities often obstruct signals, leaving users with poor quality of service (QoS), which often cannot even support basic web applications and processes. However, UAVs have the potential to solve this problem by increasing coverage and capacity in areas where traditional methods fall short [5].

New UAV-aided communication networks have been introduced [6] to address limited coverage and connectivity in dense urban areas during rush hours or emergencies. These networks consist of multiple UAVs and drones swarms that relay signals [7], mitigate multipath, and provide direct Line of Sight communication links. UAVs are crucial in disaster recovery as they create airborne backhaul networks when existing networks fail [8]. However, UAV communications rely on Radio Frequency (RF) signals, which can be susceptible to tampering, jamming, eavesdropping, and interference. The environment can also affect RF communications, with densely populated areas with tall buildings potentially blocking the direct LoS, causing partial or total signal loss.

In this paper, a Nakagami-*m* distribution-based, closed-form channel model has been introduced to capture the wireless medium behaviour with more accuracy. Additionally, the system capacity has been boosted with the deployment of a UAV along with the secrecy capacity that has been characterized for modern wireless communication systems in a dense urban environment in the presence of eavesdroppers as in Fig 1. Last, an estimation of the outage probability of the proposed system takes place, giving a higher degree of freedom to the network by following specifications compliant with the 3rd Generation Partnership Project standards for the latest generation technologies to provide a more realistic approach to channel modelling for enhanced security and capacity performance in UAV-aided networks.

II. System Analysis and Overview

Several studies have investigated the effects of blockage on UAV-to-ground communication in urban environments [9]. One study analyzed the signal attenuation and shadowing effects caused by buildings and found that the Received Signal Strength (RSS) of the communication link is significantly reduced in urban environments compared to open areas. To combat blockage in UAV-to-ground (UAV2G) communication, several techniques have been suggested. One strategy involves using relaying nodes, such as other UAVs or ground vehicles, to extend the communication range and circumvent obstacles. These techniques can prove beneficial in various environments

This work was supported by the UKRI/EPSRC SWAN Prosperity Partnership (EP/T005572/1).

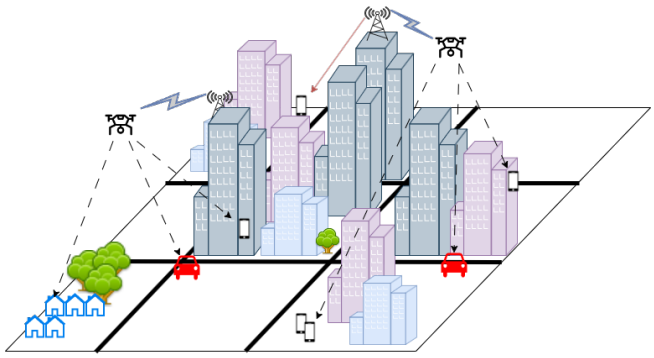

Fig. 1. Modern City UAV Deployment Scenario

and terrains, including those where adversaries may be present, by helping to mitigate poor QoS scenarios. Our work is based on two system models that use UAVs to increase the performance of the communication links between a ground-based transmitter (Tx) and a ground-based receiver (Rx) in urban, suburban, and dense urban environments. In the first case, UAV(s) act as friendly jammers aiming to boost the signal strength and enhance the secrecy of the transmission link preventing the eavesdroppers from intercepting and successfully acquiring the message [1]. This work is based on predicting the probability of achieving LoS air-to-ground (A2G) communication links between the UAV (Tx), jammer (UAV), and BS/ Ground Antenna (Rx) assuming the ground link (Tx-Rx) is facing log-distance path loss and Rayleigh fading as shown in (1). This replaces an older approximation of LoS probability provided by Sigmoid-based fitting with a piecewise-based method. Their respective channel model depicted in (1) considers the power received to be equal to the product of the transmitted power with the exponentially distributed channel power gain [1] with unit mean and β as the path loss exponent. However, the Rayleigh distribution is not the most accurate for real-time scenarios as it only accounts for many random NLoS transmission paths, without considering LoS paths, which is very improbable in real-life application scenarios including UAVs [10]. Moreover, Rayleigh channel modeling used in a free space LoS communication plane [1], is impractical due to the specific characteristics of free space propagation; distance-related only path loss.

$$P_{sd} = P_s(\lambda/4\pi)^2 \cdot l_{s,d}^{-\beta} |h_{s,d}|^2 \tag{1}$$

When compared to the Rayleigh distribution, the Nakagami-m distribution frequently offers a superior fit to measured channel data. Especially in scenarios where the signal strength is moderate to high, it is important to note that the Rayleigh distribution may overestimate the degree of fading. In cases where wireless signals encounter a combination of direct and reflected paths, the Nakagami-m distribution proves to be a more accurate representation of their behaviour compared to the Rayleigh distribution [11]. This is due to the Nakagami-m distribution's ability to take into account the varying strengths of each individual path, whereas the Rayleigh distribution assumes equal strength across all paths.

The second case involves utilizing unmanned aerial vehicles (UAVs) flying at various heights in rectangular patterns above a highly populated urban area [9]. This example illustrates how UAVs can establish a LoS communication link with ground users by following a precise rectangular pattern above buildings as if they were navigating an airborne route that mirrors the street layout below. The research includes case studies on the channel's secrecy capacity and the system's outage probability for a communication link between an operating Long Term Evolution (LTE) BS and a UAV. This link is established within a microcell located in a densely populated urban environment where eavesdroppers are randomly positioned in the air.

As a part of our work, we have introduced an airborne eavesdropper while completely removing the friendly airborne UAV jammers. This way, there is no friendly signal boosting for the transmitted signal except for the relay provided by the UAV node itself in the next stage of the communication. To simulate a dense urban microcell environment where LoS is maintained and the distance between the legitimate UAV and ground BS is a uniform random variable between 0 and 400 meters. We have also assumed that the Ground-to-Air (G2A) communication behaves like an NLoS link in terms of fast and slow far-field fading as in (2) and (3) due to reflections and multipath created by the dense urban setting. To determine the necessary parameters and factors for channel modelling, we have followed the guidelines of 3GPP specifications [4].

$$PL_{dB} = -55.9 + 38\log_{10}(d) + \left(24.5 + \frac{1.5fc}{925}\log_{10}(fc)\right) \tag{2}$$

and

$$PL_{dB} = -35.4 + 26\log_{10}(d) + 20\log_{10}(fc) \tag{3}$$

A. Channel Model Design

Although Nakagami fading is not specifically intended for LoS communication, it can still be utilized in situations where multipath effects are present. However, for scenarios where there is a clear LoS path with little to no environmental blockage or congestion, other models that explicitly consider direct LoS may be more suitable.

B. Transmitter

In this scenario, a commercially available cellular network's LTE-5G BS functions as the transmitter (Tx). The UAV (Rx) connects to the network like any other User Equipment (e.g. mobile phone) and receives the same radio frequency (RF) service. We assume that the cellular BS uses a 4-by-4 patch antenna array that operates at a frequency of 2.4 GHz, with a maximum antenna gain of 18.8 dBi. The antenna's main lobe beamforms to maintain alignment with the UAV at all times, regardless of the eavesdropper's position alignment with the antenna.

TABLE I
BS ANTENNA ARRAY METRICS

Parameter	Value
Half Power Beam Width (HPBW)	30.0°
First Null Beam Width (FNBW)	60.0°
Front to Back Ratio (F/B)	24.4 dB
Sidelobe Level (SLL)	18.4 dB
Main	18.8 dB
Back	-5.58 dB

C. Receiver

The drone/UAV (Rx) used in our simulations operates similarly to any commercially available drone intended for urban use. It stays connected through the cellular network and flies within the main lobe of the radiated pattern. It has an omni-directional receiving antenna with a gain of 2 dBi and can operate within a maximum range of 500 m. The eavesdroppers in our experiment have the same performance capabilities as the legitimate UAV, with the only difference being their positioning. They can be placed anywhere within a 400-by-400 m^2 area around the BS and the UAV, with the BS at the centre of the area O(0,0). All airborne units are assumed to operate at the same altitude.

$$f(x) = \frac{2m}{\Gamma(m)} \left(\frac{x}{m}\right)^{2m-1} \exp\left(-\frac{x^2}{m}\right) \tag{4}$$

$$f(x) = \frac{2m}{\Gamma(m)} \left(\frac{x}{m}\right)^{2m-1} \exp\left(-\frac{x^2}{m}\right) \times \frac{1}{\sigma_{\text{dB}}\sqrt{2\pi}} \exp\left(-\frac{(10\log_{10}x - \mu_{\text{dB}})^2}{2\sigma_{\text{dB}}^2}\right) \tag{5}$$

Furthermore, we have modeled the system based on the assumption that the UAV's route begins from a LoS position of 50 m away from the BS, and gradually increases its distance to a maximum distance of up to 650 m away. The LoS state positions are only subject to path loss caused by distance and environmental noise, related to temperature conditions. In expression 5, x is the instantaneous amplitude of the received signal, m is the fading parameter of the Nakagami-m distribution, $\Gamma(m)$ is the gamma function, σ_{dB} and μ_{dB} are the standard deviation and mean of the log-normal shadowing, respectively, and $10 \times \log_{10}(\text{x})$ is the signal strength in decibels (dB). The expression is used to calculate the probability density function of the received signal amplitude in a dense urban environment.

III. ANALYTICAL RESULTS

The first stage of the research was to determine which mathematical model would be more practical and realistic for the simulated scenario and which scenario would provide enough details to describe the fading factors affecting the communication channel. Most studies available focus exclusively on Rayleigh channels when it comes to NLoS cases and Rician when it comes to pure LoS cases. It is more appropriate to use Nakagami-m channel model to provide a greater degree of flexibility and describe more accurately a scenario where LoS communication is achieved, but at the same time is affected by severe fading due to dense urban environmental obstructions. It introduces a shape parameter that allows more flexibility in modelling the fading severity. When the shape parameter is equal to 1, the Nakagami model reduces to the Rayleigh model, whereas when is greater than 1, represents a fading environment with more LoS characteristics, resembling a Rician model.

In order to define the best m parameter for the Nakagami channel model, rigorous simulation testing has been employed. These results, together with simulations to validate the mathematical channel model are presented in the next section.

For our case, it is assumed the distance of both the legitimate UAV and eavesdroppers follows a uniform distribution with predetermined lower and maximum values. The BS transmitting power is a constant value, along with the receiver's antenna gain G_r and the system's noise figure N_o caused by the atmospheric temperature. The achievable transmitter's gain G_t is dependent on the relative position of the receiver to the BS antenna array with a range of values as shown in table I. The channel gain G_c of our described system follows Nakagami distribution and the related PDF of the gain is depicted in (6):

$$\textit{Nakagami PDF} : f(x;m,\Omega) = \frac{2m^m}{\Gamma(m)\Omega^m} x^{2m-1} \exp^{-\frac{m}{\Omega}x^2} \tag{6}$$

However, the channel coefficient G_c^2 follows a Gamma distribution with shape parameter $k = 2$ and scale parameter $\theta = 1/2$, derived from Nakagami parameters relations of $m = 2$ and $\omega = 1$. Hence the Γ distribution parameters will relate as $k = m$ and $\theta = \omega/m$. The probability density function (PDF) of this Gamma distribution is:

$$f(x) = \frac{x^{k-1}\exp^{-\chi/\theta}}{\theta^k \times \Gamma(k)} \tag{7}$$

which for this specific scenario the PDF of Γ distribution will be formed as:

$$f(x) = 4x\exp^{-2x} \tag{8}$$

The CDF of the Γ distribution for the parameters of $k = 2$ and $\theta = 1/2$ is:

$$F(x) = \begin{cases} \Gamma(2, \frac{1}{2}) & \text{if } x > 0, \\ 0 & \text{otherwise} \end{cases} \tag{9}$$

The Nakagami PDF is:

$$f(x) = 8x^3\exp(-2x^2) \tag{10}$$

Legitimate and Wiretap Channel Capacity [12]:

$$C_x = \mathbb{E}[\log_2(1 + SNR_x)] \tag{11}$$

Average Legitimate and Wiretap Channel Capacity over the fading distribution:

$$\mathbb{E}[\log_2(1 + SNR_x)] = \int_{-\infty}^{\infty} \log_2(1 + SNR_x) \times PDF \tag{12}$$

Substituting the expression for SNR_m into the integral, we get:

$$C_s = \int_{-\infty}^{\infty}\int_{-\infty}^{\frac{d^4 No(\exp(z)-1)}{Pt}} \frac{4x\exp(-2x)}{d_{max}-dmin}\,dx\,dd \Rightarrow$$

$$C_s = \int_{-\infty}^{\infty}\int_{0}^{\frac{d^4 No(\exp(z)-1)}{Pt}} \frac{4x\exp(-2x)}{d_{max}-d_{min}}\,dx\,dd \Rightarrow$$

$$C_s = \int_{d_{min}}^{d_{max}}\int_{0}^{\frac{d^4 No(\exp(z)-1)}{Pt}} \frac{4x\exp(-2x)}{d_{max}-d_{min}}\,dx\,dd \qquad (13)$$

where $d_{max} > d_{min} \geq 0$ *and* $\{d_{min}, d_{max}\} \in \mathbb{R}$. Distance is assumed to follow a uniform distribution so d is uniformly distributed between d_{min} and d_{max}. When these assumptions are taken into account, the double integral from above can be further simplified to:

$$\begin{aligned}
C_s &= d_{max} - d_{min} + \frac{1}{8\times 2^{\frac{1}{8}} Pt^2} \\
&\times \left[-Pt^2 \left\{ \frac{d_{max}\left(\Gamma\left(\frac{1}{8}\right) - \Gamma\left(\frac{1}{8}, \frac{2d_{max}^8(-1+\exp(z)^2 No^2}{Pt^2}\right)\right)}{\left(\frac{d_{max}^8(-1+\exp(z)\times No^2)}{Pt^2}\right)^{\frac{1}{8}}} \right.\right. \\
&\left.\left. + \frac{d_{min}\left(-\Gamma\left(\frac{1}{8}\right) + \Gamma\left(\frac{1}{8}, \frac{2d_{min}^8(-1+\exp(z)^2 No^2}{Pt^2}\right)\right)}{\left(\frac{d_{min}^8(-1+\exp(z)\times No^2)}{Pt^2}\right)^{\frac{1}{8}}} \right\} \right. \\
&- (-1+\exp(z))^2 No^2 \\
&\times -Pt^2 \left\{ \frac{d_{max}^9\left(\Gamma\left(\frac{9}{8}\right) - \Gamma\left(\frac{9}{8}, \frac{2d_{max}^8(-1+\exp(z))^2 No^2}{Pt^2}\right)\right)}{\left(\frac{d_{max}^8(-1+\exp(z)\times No^2)}{Pt^2}\right)^{\frac{9}{8}}} \right. \\
&\left.\left. - \frac{d_{min}^9\left(\Gamma\left(\frac{9}{8}\right) - \Gamma\left(\frac{9}{8}, \frac{2d_{min}^8(-1+\exp(z))^2 No^2}{Pt^2}\right)\right)}{\left(\frac{d_{min}^8(-1+\exp(z)\times No^2)}{Pt^2}\right)^{\frac{9}{8}}} \right\} \right] \Rightarrow
\end{aligned}$$

$$\begin{aligned}
C_s &= \frac{1}{128}\left\{ 16 d_{max}\left(8 + \exp^{\frac{-2d_{max}^8(-1+\exp(z))^2 No^2}{Pt^2}}\right) \right. \\
&+ 16 d_{min}\left(-8 - \exp^{\frac{-2d_{min}^8(-1+\exp(z))^2 No^2}{Pt^2}}\right) \\
&+ 18 d_{max}\mathrm{Ei}\left[\frac{7}{8}, \frac{2d_{max}^8(-1+\exp(z))^2 No^2}{Pt^2}\right] \\
&- \frac{9\times 2^{\frac{7}{8}} d_{max}\Gamma\left(\frac{1}{8}\right)}{\left(\frac{d_{max}^8(-1+\exp(z)\times No^2)}{Pt^2}\right)^{\frac{1}{8}}} \\
&\left. + \frac{9\times 2^{\frac{7}{8}} d_{min}\left(\Gamma\left(\frac{1}{8}\right) - \Gamma\left(\frac{1}{8}, \frac{2d_{min}^8(-1+\exp(z))^2 No^2}{Pt^2}\right)\right)}{\left(\frac{d_{min}^8(-1+\exp(z)\times No^2)}{Pt^2}\right)^{\frac{1}{8}}} \right\} \qquad (14)
\end{aligned}$$

IV. Simulation Results

Simulations based on the 3GPP standards for LTE-A and 5G systems were conducted to validate the derivation of Signal-to-Noise Ratio and path loss analysis across different channel

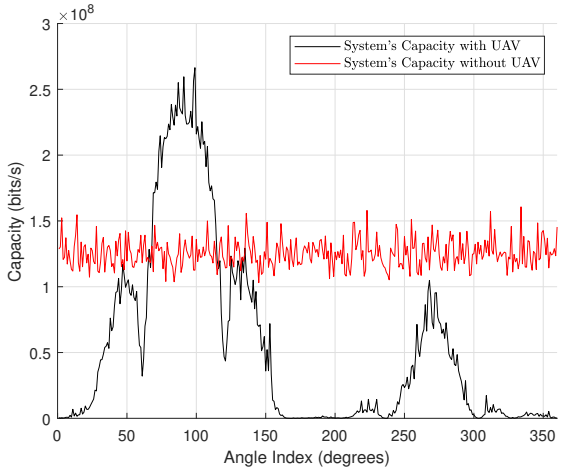

Fig. 2. System's Capacity comparison in the presence of a UAV and without

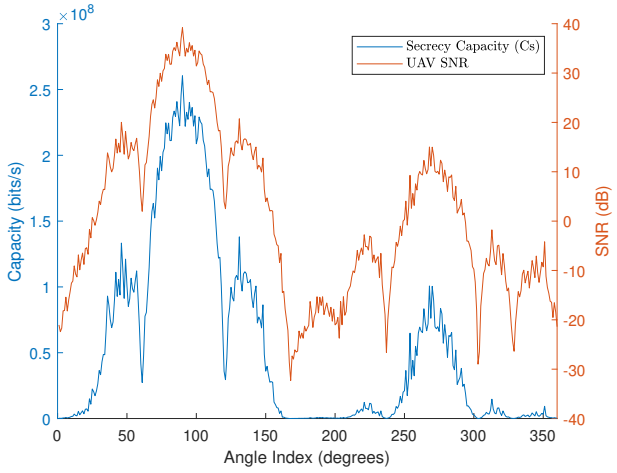

Fig. 3. System's Secrecy Capacity and SNR for the UAV at a distance of 400m around the BS

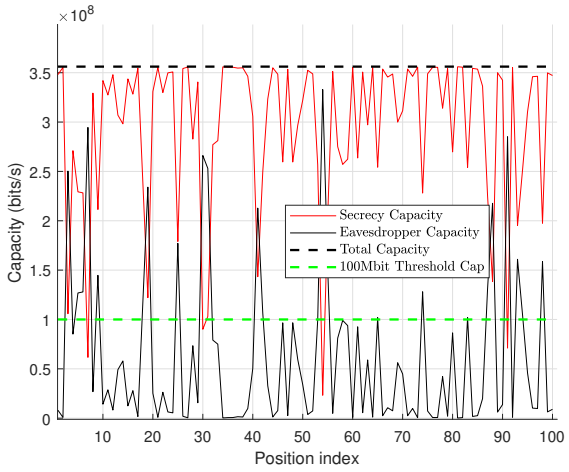

Fig. 4. Secrecy Capacity (Cs) against eavesdropper's Capacity, with a minimum operational capacity of 100 Mbit/s

models along with the system's performance in the presence and absence of a UAV was compared. Unless specified otherwise, all system parameters used in the simulations are listed in Table II. Moreover, our work focused on the secrecy capacity and outage probability achieved when the UAV was deployed as seen in Table III. It has been tested for distances of 50 m up to 650 m around the BS, with the criterion being the Secrecy Capacity of the legitimate link being lower to the wiretap link $Cs_{\text{legit}} \leq C_{wt}$ over multiple iterations. Furthermore, a closed-form solution for calculating the channel's secrecy capacity was proposed previously based on the optimal m factor selected. During each trial of the simulation, sets of positions are generated from 50 m away from the transmitting BS, all the way up to 650 m away, representing the locations of the UAV distance to the BS location. For every position of the UAV, a channel model is generated calculating the instantaneous path loss, received power at the relay node (UAV), and the link's SNR, which is characterized by the random statistics the Nakagami-m coefficients offer to the channel in those locations denoting the fading effects occurring in the signal propagation. Where LoS communication is achieved, the communication channel is only subject to distance-related path loss, and environmental thermal noise. Afterwards, a reference average SNR is estimated based on all the instantaneous SNRs generated in every trial, along with the fading caused by path loss, the capacity of the network system, and the outage probability as mentioned earlier. In order for the available data rate for the communication link to be estimated, Shannon's formula is employed. This confirms that a reliable and fast enough [13] [14] data rate connection even in heavily fading affected cases with lower SNRs can now get established. As a result, previously signal-dead or low capacity areas in the city are now serviced meeting the requirements for deployment of more intensive applications as shown in Fig. 2. It is evident in Fig. 3 that by deploying a UAV to service a focused location, with simple beam forming, almost 100 Mbit/s of additional capacity can be provided, increasing QoS while simultaneously preventing nearby eavesdroppers capturing data from any direction.

In Fig. 4, the Secrecy capacity (C_s), the eavesdropper capacity, the system's maximum capacity and a 100 Mbit/s minimum operational capacity threshold are depicted, against a position index. The positions are random uniformly generated reference positions and all have the same simulation characteristics. In order to estimate the relevant capacities for each position, distance-related pathloss, fading, and SNR are used. The red line describes the Secrecy Capacity (C_s) is fluctuation against the eavesdropper's capacity (black solid line) for 100 different eavesdropper positions. It is clear that only in very rare cases the (C_s) drops lower than the 100 Mbit threshold capacity that is set as the minimum operational capacity. This provides the system with enough resources to support various applications [14]. The higher available Cs in the system provided by the UAV implementation provides larger service capacity to users, where previously was limited. With further investigation, our work has achieved a minimum

TABLE II
SYSTEM SIMULATION PARAMETERS

Parameter	Value
Environment	Dense Urban
Flying range	[50 650] m
LoS distance breakpoint	300 m
Tx / Rx gain	1 dBi
Carrier Frequency	2.4 GHz
Spectrum allocation Bandwidth	20 MHz
Thermal noise power density	-174 dBm/Hz
Path loss exponent	4
Transmit power	10W

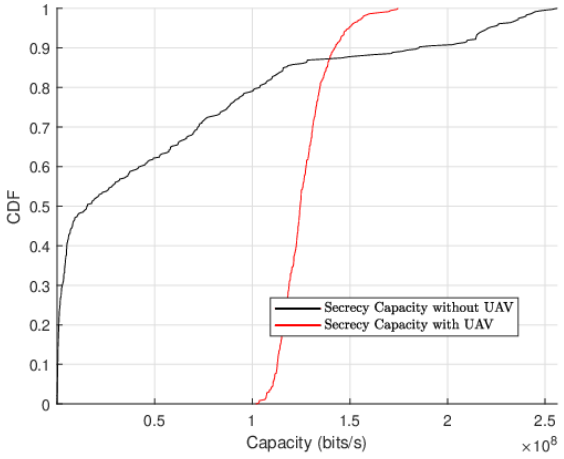

Fig. 5. Secrecy Capacity (Cs) CDF comparison in the presence of UAV and without

C_s of 60 Mbit/s in those areas as seen in Fig. 4, which can be more than enough for basic needs and potentially higher demanding data rate applications to be made feasible.

It is evident that while the UAV can sustain a communication link with the BS, there is no significant loss of signal strength or risk of a network failure that could undermine the security, dependability, and universality of the network at any given moment.

In order to prove the resilience of our system model against outages and low performance, we have conducted simulations and calculated the system's outage probability under various scenarios. We have derived the outage probabilities for our system based on a specific m parameter that we believe suits best our system, demonstrating that even at the worst-case scenario of complete NLoS at the maximum distance of 650 m, our UAV-aided network implementation outperforms the non-UAV one, as shown in table III. For shorter NLoS operating distances of up to 450 m, although in an NLoS state after the breakpoint of 300 m, the probability of experiencing a system outage is very low ($\sim$0.3-1.5%) depending on the relative positions of the eavesdropper with regards to the UAV position and BS. For longer NLoS distances ($>$ 550 m) the UAV system experiences an increased danger of outages as expected, however, in a dense urban setup like ours, distances of this scale or greater between the UAV and the BS, will

TABLE III
SYSTEM OUTAGE PROBABILITY (AVG.)

distance (m)	with UAV	without UAV
350	0.003	0.080
450	0.015	0.120
550	0.095	0.154
650	0.153	0.33

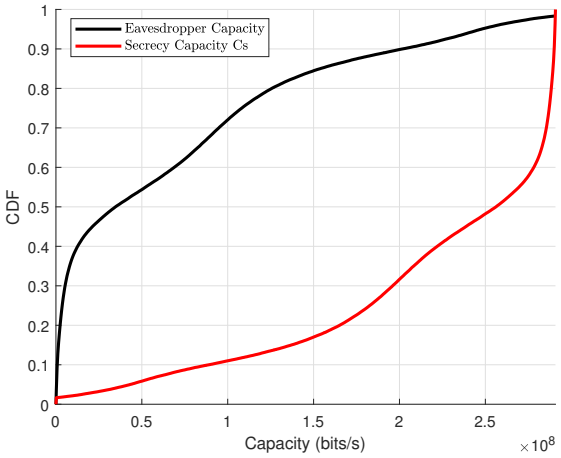

Fig. 6. System's Secrecy Capacity relative to eavesdroppers performance

very rarely occur, as modern networks layout and planning enable quick handovers after shorter distances, meaning that as long as the UAV maintains an aligned positioning to the BS mainlobe, the eavesdropping possibilities causing outages will be minimal.

These are confirmed by the fact the UAV presence creates a significantly higher overall capacity for the network compared to not having a UAV, as seen in Fig. 5 meaning outages are becoming a rarity and service availability more possible. Furthermore, even in the presence of an eavesdropper, the UAV is still able to enhance the available C_s of the system, by maintaining a minimum secrecy capacity of at least 50 Mbit/s in $\sim$99% of the cases as displayed in Fig. 6, regardless of the eavesdropper's achieved capacity.

V. Conclusions

This work proposes a novel application of Nakagami-*m* channel modeling for ground-to-air communications in dense urban environments, in the presence of an active eavesdropper. In particular, by implementing this method in highly faded application scenarios as this one, we introduce NLoS propagation characteristics to the system simulating a worst-case scenario caused by path loss and fading. Our proposal comprises a closed-form solution that more accurately captures the fluctuation of the secrecy capacity of the studied system. Specifically, our method tests the system C_s change in the presence of an airborne eavesdropper with and without a friendly UAV. The friendly UAV employment achieves almost 6 times more reliable communication by minimizing the cases where the network experiences outages and also providing robust transmission where previously there was 60% probability of the system achieving $C_s \leq 50$ Mbit/s. Moreover, the system provides double the C_s it used to, for the cases it used to suffer from reduced C_s. However, the system experiences a limited potential for Capacity increase, as it is affected by distance and relay-induced losses compared to the case with no UAV employed. This could be mitigated by deploying additional friendly UAVs with intelligent placement algorithms and by forming an airborne mesh network capacity and throughput could be further increased significantly.

References

[1] J. Tang, G. Chen, and J. P. Coon, "Secrecy performance analysis of wireless communications in the presence of UAV jammer and randomly located UAV eavesdroppers," *IEEE Trans. on Inf. Forensics Security*, vol. 14, pp. 3026–3041, Nov. 2019.

[2] M. Z. I. Sarkar, T. Ratnarajah, and M. Sellathurai, "Secrecy capacity of Nakagami-m fading wireless channels in the presence of multiple eavesdroppers," in *2009 Conference Record of the Forty-Third Asilomar Conference on Signals, Systems and Computers*, pp. 829–833, IEEE, 2009.

[3] S. Dang, O. Amin, B. Shihada, and M.-S. Alouini, "What should 6G be?," *Nat. Electron.*, vol. 3, pp. 20–29, Jan. 2020.

[4] 3GPP *Spatial channel model for Multiple Input Multiple Output (MIMO) simulations (Release 17)*, 3GPP TR 25.996, Mar. 2022.

[5] M. Ayamga, S. Akaba, and A. A. Nyaaba, "Multifaceted applicability of drones: A review," *Technological Forecasting and Social Change*, vol. 167, 2021.

[6] S. Yang, D. Shi, Y. Peng, W. Qin, and Y. Zhang, "Joint communication-motion planning for UAV relaying in urban areas," in *Proc. Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)*, (Rome, Italy), pp. 1–9, July 2021.

[7] S. K. Khan, U. Naseem, A. Sattar, N. Waheed, A. Mir, A. Qazi, and M. Ismail, "UAV-aided 5G network in suburban, urban, dense urban, and high-rise urban environments," in *Proc. IEEE 19th International Symposium on Network Computing and Applications (NCA)*, (Cambridge, MA, USA), pp. 1–4, Nov. 2020.

[8] M. Gapeyenko, V. Petrov, D. Moltchanov, S. Andreev, N. Himayat, and Y. Koucheryavy, "Flexible and reliable UAV-assisted backhaul operation in 5G mmWave cellular networks," *IEEE J Sel. Areas Commun.*, vol. 36, pp. 2486–2496, Nov. 2018.

[9] Z. Yang, L. Zhou, G. Zhao, and S. Zhou, "Blockage modeling for Inter-layer UAVs communications in urban environments," in *Proc. IEEE International Conference on Telecommunications (ICT)*, pp. 307–311, Jun. 2018.

[10] S. Belmoubarik, G. Aniba, and B. Elgraini, "Secrecy capacity of a Nakagami-m fading channel in the presence of cooperative eavesdroppers," in *Proceedings of 2014 Mediterranean Microwave Symposium (MMS2014)*, pp. 1–6, IEEE, 2014.

[11] T.-T. T. Dao, S. Q. Nguyen, H. Nhung-Nguyen, P. X. Nguyen, and Y.-H. Kim, "Performance evaluation of downlink multiple users NOMA-enable UAV-aided communication systems over Nakagami-m fading environments," *IEEE Access*, vol. 9, pp. 151641–151653, Oct. 2021.

[12] Z. Abdullah, G. Chen, M. A. M. Abdullah, and J. A. Chambers, "Enhanced secrecy performance of multihop IoT networks with cooperative hybrid-duplex jamming," *IEEE Trans. Inf. Forensics and Security*, vol. 16, pp. 161–172, Jun. 2020.

[13] K. Liolis, J. Cahill, E. Higgins, M. Corici, E. Troudt, and P. Sutton, "Over-the-air demonstration of satellite integration with 5G core network and multi-access edge computing use case," in *Proc. IEEE 2nd 5G World Forum (5GWF)*, pp. 1–5, Sep. 2019.

[14] V. Petrov, D. Solomitckii, A. Samuylov, M. A. Lema, M. Gapeyenko, D. Moltchanov, S. Andreev, V. Naumov, K. Samouylov, M. Dohler, and Y. Koucheryavy, "Dynamic multi-connectivity performance in ultra-dense urban mmWave deployments," *IEEE J Sel. Areas Commun.*, vol. 35, no. 9, pp. 2038–2055, Sep. 2017.