Trustworthy Slotted ALOHA

Apostolos A. Tegos, Yue Xiao, Sotiris A. Tegos, *Senior Member, IEEE,*
George K. Karagiannidis, *Fellow, IEEE,* and Panagiotis D. Diamantoulakis, *Senior Member, IEEE*

***Abstract*—Meeting the ever-increasing demands for trustworthy wireless communication is crucial in modern networks. In this work, we investigate physical layer security in a slotted ALOHA scheme with randomly distributed users. Specifically, we evaluate a system where users are randomly distributed in a ring around the base station (BS), while eavesdroppers are distributed in rings around them. We propose that legitimate users allocate a fraction of their transmit power to generate artificial noise (AN) to increase the probability of secure transmission. To evaluate the performance of the proposed trustworthy slotted ALOHA scheme, we introduce a new metric called secrecy outage rate and derive a closed-form expression for this metric, which involves the outage probability at both the BS and the eavesdropper. Simulation results validate the theoretical analysis and demonstrate the superiority of the proposed scheme over a benchmark scheme without AN, as well as the usefulness of the proposed metric.**

***Index Terms*—physical layer security, trustworthiness, random access, slotted ALOHA, artificial noise, secrecy outage rate, 6G**

I. Introduction

TRUSTWORTHINESS-by-design has been a high priority in sixth generation wireless networks to increase the level of protection against security risks such as malicious forwarding, tampering, and eavesdropping. Although trustworthiness [1] can be improved by using upper-layer techniques, such as advanced encryption, this is very challenging in internet-of-things (IoT) networks due to the limited computational complexity of the transmitters. Therefore, physical layer security (PLS) is an interesting alternative technique for IoT networks. The study of security in wireless communications was initiated in [2], which introduced the wiretap channel model and proved that proper coding can ensure reliable and secure data transmission. More recently, researchers have focused on PLS with the goal of using the characteristics of the communication channel, such as channel fading and noise, to generate encryption keys to secure transmitted data [3]. PLS can also be used to provide information-theoretic secrecy [4] or covert communication [5] by preventing decoding or obtaining the user's message, respectively. However, only a limited number of papers have investigated PLS for IoT networks, where contention-based medium access, such as slotted ALOHA, is the dominant technology.

In more detail, a widely used technique to ensure secrecy and covert communication is the insertion of artificial noise (AN) into the eavesdropper's channel to ensure that the channel between the base station (BS) and the legitimate user (LU) is superior. In [6], AN was used to ensure secrecy, and different scenarios were studied, considering both single and multiple antennas in the transmission as well as in the eavesdroppers. Furthermore, in [7], secure transmission in a channel-aware random access system was investigated. Taking advantage of the known channel state information (CSI) in the channel-aware system, opportunistic jamming was implemented to increase the secrecy rate. For example, active users that do not transmit data in a particular time slot transmit random signals to disrupt the eavesdropper. Finally, in [8], the authors proposed that the AN is generated by the BS, which degrades the eavesdropper's channel, while it can be cancelled by the LU due to prior knowledge. However, existing metrics are not suitable to describe the quality-of-service in slotted ALOHA, when the LU transmits jamming signals simultaneously with the transmitted data to degrade the eavesdropper's channel. Also, performing resource allocation by focusing only on throughput or ignoring the use of AN is expected to lead to suboptimal solutions.

Motivated by the above, we introduce a trustworthy slotted ALOHA (TS-ALOHA) scheme for networks with randomly distributed users. The proposed scheme, which is implemented at the physical layer, neither increases the computational complexity nor requires the availability of CSI at the transmitter side. Specifically, we focus on the analysis of an uplink communication network where LUs are randomly and uniformly distributed in a ring around the BS, while eavesdroppers are located in circular rings around the LUs. We propose that the active user allocates a fraction of the transmit power to generate AN in order to degrade the channel conditions of the eavesdropper. We assume that the AN is known to the BS and can be cancelled during decoding. To evaluate the performance of the system and assess the impact of its inherent characteristics, we propose a new metric, the *secrecy outage rate*. This metric takes into account not only the probability of outage, but also factors such as transmission rate, access probability, and random access collisions, and is tailored for random access networks. Closed-form expressions for the secrecy outage rate are derived by first extracting closed-form expressions for the outage probability at the BS and the eavesdropper. The theoretical analysis is validated by simulation results, where we aim to maximize the secrecy outage rate by appropriately allocating the system resources, providing useful insights into the selection of the access probability and the fraction of the transmit power for AN.

A. A. Tegos is with the Department of Electrical and Computer Engineering, Aristotle University of Thessaloniki, 54124 Thessaloniki, Greece (e-mail: apotegath@auth.gr).

Y. Xiao is with the Provincial Key Laboratory of Information Coding and Transmission, Southwest Jiaotong University, Chengdu 610031, China (e-mail: alice_xiaoyue@hotmail.com)

S. A. Tegos, G. K. Karagiannidis and P. D. Diamantoulakis are with the Department of Electrical and Computer Engineering, Aristotle University of Thessaloniki, 54124 Thessaloniki, Greece and with the Provincial Key Laboratory of Information Coding and Transmission, Southwest Jiaotong University, Chengdu 610031, China (e-mails: tegosoti@auth.gr, geokarag@auth.gr, padiaman@auth.gr).

This work was supported by NSFC 62350710217 and Sichuan HT 2024JDHJ0042. The work of Y. Xiao was supported by CPSF 2023TQ0278 amd Postdoctoral Fellowship Program of CPSF-B GZB20230613.

This article has been accepted for publication in IEEE Wireless Communications Letters. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/LWC.2024.3468469

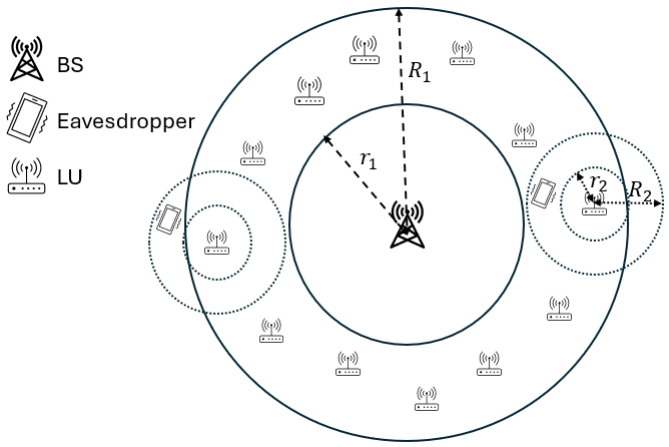

Fig. 1. System model.

II. System Model

We consider a secure uplink communication between a BS and N LUs randomly deployed around the BS, while an eavesdropper attempts to detect and decode the communication. All nodes are assumed to be equipped with a single antenna. The LUs are assumed to be randomly distributed in a ring centered around the BS, while an eavesdropper is randomly distributed around each LU in a ring, as shown in Fig. 1. Given that the LUs are uniformly distributed in a circular ring centered around the BS with inner radius r_1 and outer radius R_1, the distance d_i between the i-th LU and the BS is a random variable with cumulative distribution function (CDF) given by

$$F_{d_i}(x) = \frac{x^2 - r_1^2}{R_1^2 - r_1^2},\ x \in [r_1, R_1], \tag{1}$$

while the probability density function (PDF) is expressed as

$$f_{d_i}(x) = \frac{2x}{R_1^2 - r_1^2},\ x \in [r_1, R_1]. \tag{2}$$

Regarding the eavesdroppers, to improve the system performance, we consider an exclusion zone around the LUs [9], thus each eavesdropper is distributed in a circular ring around each LU. Similarly, the PDF of the distance d_j between the LU and its respective eavesdropper is given by

$$f_{d_j}(x) = \frac{2x}{R_2^2 - r_2^2},\ x \in [r_2, R_2], \tag{3}$$

where R_2, r_2 denote the outer and inner radius of the ring of the eavesdropper, respectively.

III. TS-ALOHA and Secrecy Outage Rate

We introduce a TS-ALOHA scheme, since slotted ALOHA [10] has been shown to outperform other random access protocols, and we propose the use of AN to improve the system performance. Specifically, the LUs transmit their signals in specific time slots and the i-th LU accesses the channel with a predetermined access probability q_i. With respect to the AN, the LUs simultaneously use a fraction of the transmit power to generate a random signal in order to interfere with the existing eavesdroppers and ensure the secrecy of the messages. Specifically, we assume that the LU allocates a fraction α of its transmit power to transmit the message and the rest $(1-\alpha)$ to transmit the AN. This random signal, generated by the LU, is known to the BS, which is able to separate it from the superimposed signal and decode the transmitted message without any additional noise from it. Taking this into account, the signal-to-noise ratio (SNR) received by the BS from the i-th source is given by

$$\gamma_i = \frac{\alpha l_i |h_i|^2 p_i}{\sigma^2}, \tag{4}$$

where σ^2, h_i, and p_i denote the variance of the additive white Gaussian noise (AWGN), the small scale fading coefficient between the i-th LU and the BS, and the transmit power of the i-th source, respectively, while l_i is the path loss factor and is expressed as

$$l_i = c d_i^{-n}, \tag{5}$$

where c is the path loss at reference distance d_0 and n denotes the path loss exponent. Regarding the eavesdroppers, the received SNR is given by

$$\gamma_j = \frac{\alpha l_j |h_j|^2 p_i}{(1-a) l_j |h_j|^2 p_i + \sigma^2}, \tag{6}$$

where h_j denotes the small-scale fading coefficient between the i-th LU and the eavesdropper, and $l_j = c d_j^{-n}$ with d_j being the distance between the i-th LU and the eavesdropper around it. Assuming Rayleigh fading, $|h_i|^2$ and $|h_j|^2$ follow the exponential distribution with rate parameter 1.

A parameter that significantly affects the system performance is the transmission rate. In this work, a fixed transmission rate is investigated. Specifically, when a LU accesses the channel the achievable rate for the i-th source is given by

$$\tilde{R}_i = B \log_2(1 + \gamma_i), \tag{7}$$

where B is the available bandwidth. We consider a fixed target rate denoted as $\hat{R}_i$. When the channel conditions deteriorate and such a rate cannot be achieved, i.e., $\tilde{R}_i < \hat{R}_i$, an outage occurs. In this direction, the SNR threshold for the decoding of the message of the i-th LU at both the BS and the eavesdropper is given by

$$\beta_i = 2^{\frac{\hat{R}_i}{B}} - 1. \tag{8}$$

To accurately evaluate the performance of the system, we propose a new metric called *secrecy outage rate*. This metric combines the target rate, the access probability of each LU, the complementary outage probability at the BS, which is the probability that the BS can correctly decode the transmitted message, and the outage probability at the eavesdropper, which is the probability that the eavesdropper is unable to decode the transmitted message.

Theorem 1: The secrecy outage rate of the i-th LU is given by

$$\tilde{R}_i = \hat{R}_i (1 - P_i) P_j q_i \prod_{k \neq i} (1 - q_k), \tag{9}$$

where P_i is the outage probability at the BS, and P_j is the outage probability at the eavesdropper. The outage probability at the BS is given by

$$P_i = \frac{2}{R_1^2 - r_1^2} \left(\frac{\gamma\left(\frac{2}{n}, \frac{\sigma^2 \beta_i R_1^n}{a c p_i}\right)}{n \left(\frac{\sigma^2 \beta_i}{a c p_i}\right)^{\frac{2}{n}}} - \frac{\gamma\left(\frac{2}{n}, \frac{\sigma^2 \beta_i r_1^n}{a c p_i}\right)}{n \left(\frac{\sigma^2 \beta_i}{a c p_i}\right)^{\frac{2}{n}}} \right), \tag{10}$$

where $\gamma(s,x)=\int_0^x t^{s-1}e^{-t}\mathrm{d}t$ denotes the lower incomplete Gamma function [11]. Regarding the system secrecy performance, we consider that the system is secure if the existing eavesdropper is unable to successfully receive the transmitted message, which is equivalent to an outage at the eavesdropper. The probability of an outage at the eavesdropper is given by

$$P_j=\frac{2}{R_2^2-r_2^2}\times\left(\frac{\gamma\left(\frac{2}{n},\frac{\sigma^2\beta_i R_2^n}{(\alpha+\alpha\beta_i-\beta_i)cp_i}\right)}{n\left(\frac{\sigma^2\beta_i}{(\alpha+\alpha\beta_i-\beta_i)cp_i}\right)^{\frac{2}{n}}}-\frac{\gamma\left(\frac{2}{n},\frac{\sigma^2\beta_i r_2^n}{(\alpha+\alpha\beta_i-\beta_i)cp_i}\right)}{n\left(\frac{\sigma^2\beta_i}{(\alpha+\alpha\beta_i-\beta_i)cp_i}\right)^{\frac{2}{n}}}\right). \tag{11}$$

Proof: The secrecy outage rate is the product of the target rate of the i-th LU with the probabilities that the BS receives the message correctly $(1-P_i)$, the eavesdropper is unable to decode the message P_j, the i-th LU accesses the channel q_i, and there is no collision $\prod_{k\neq i}(1-q_k)$ [12].

An outage occurs when the received SNR at the BS is less than the SNR threshold and is defined as

$$P_i=\Pr\left(\gamma_i<\beta_i\right). \tag{12}$$

Combining this with (2) and (4). the outage probability at the BS is given by

$$P_i=\frac{2}{R_1^2-r_1^2}\int_{r_1}^{R_1}e^{-\frac{\sigma^2\beta_i d_i^n}{\alpha cp_i}}d_i\mathrm{d}d_i. \tag{13}$$

Implementing [11, (3.381.8)], the final expression is derived.

Similar to the case of the BS, an outage at the eavesdropper occurs when the received SNR is less than the predefined threshold. The probability of this event is given by

$$P_j=\Pr(\gamma_j<\beta_i). \tag{14}$$

Taking (6) into consideration, (14) is equivalent to

$$P_j=\frac{2}{R_2^2-r_2^2}\int_{r_2}^{R_2}e^{-\frac{\sigma^2\beta_i d_j^n}{cp(\alpha+\alpha\beta_i-\beta_i)}}d_j\mathrm{d}d_j \tag{15}$$

and the proof is completed. ■

Proposition 1: It should be noted that for $\alpha\leq\frac{\beta_i}{\beta_i+1}$ an outage at the eavesdropper always occurs, which provides a useful design insight for the proposed system, since it is pointless to choose α lower than $\frac{\beta_i}{\beta_i+1}$.

Proof: Starting from (14), the outage probability at the eavesdropper is given by

$$\begin{aligned}P_j&=\Pr\left(\frac{acd_i^{-n}|h|^2p}{(1-a)cd_i^{-n}|h|^2p+\sigma^2}<\beta_i\right)\\&=\Pr\left(cd_i^{-n}|h|^2p(\alpha+\alpha\beta_i-\beta_i)<\sigma^2\beta_i\right).\end{aligned} \tag{16}$$

In (16), both the right hand side of the inequality and the term $cd_i^{-n}|h|^2p$ are positive, and thus if $\alpha+\alpha\beta_i-\beta_i\leq 0$ the inequality always stands, which proves that $P_j=1$. Considering that $\beta_i>0$, the final expression is derived. ■

IV. Numerical Results and Simulations

In this section, we illustrate the performance of the considered network and validate the theoretical analysis with simulations. We assume that $c=10^{-3}$, $n=2.5$, $\beta_i=\beta$, $\forall i$, and the total number of LUs is $N=10$ randomly distributed in a ring, centered around the BS, with inner radius $r_1=5$ m and outer radius $R_1=15$ m. Regarding the eavesdroppers, they are located in a ring with inner radius $r_2=5$ m and outer radius $R_2=10$ m centered around the active LU.

To properly allocate the resources in the considered system, we formulate and solve the following problem:

$$\begin{aligned}&\max_{\boldsymbol{p},\boldsymbol{q},\alpha}\quad \tilde{R}_i\\&\textbf{s.t.}\quad \mathrm{C}_1:\ p_iq_i\leq P_{\max},\quad \mathrm{C}_2:\ \alpha\in[0,1],\end{aligned} \tag{17}$$

where $\boldsymbol{p}$ and $\boldsymbol{q}$ denote the vectors of the active user's transmit power and each user's access probability, respectively, while C_1 is a power constraint, where $P_{\max}$ is the maximum available transmit power. By normalizing $P_{\max}$ with respect to the noise variance, we obtain the maximum SNR, which is the x-axis of the following figures.

In Fig. 2, the system secrecy outage rate is plotted against the transmit SNR for different values of β. As expected, increasing the transmit SNR leads to better system performance. In addition, the effect of varying β on system performance can be evaluated. Specifically, at low SNR, the difference in system secrecy outage rate as β changes is minimal. However, for SNR >50 dB, the system's behavior changes significantly, as higher values of β are preferred and the improvement in the secrecy outage rate becomes quite significant. This can be explained by considering that when the SNR is low enough, the system conditions are not able to support higher thresholds for correct message transmission, which results in increased outage at the BS and thus reduced secrecy outage rate. In addition, the system performance is compared to a benchmark scheme where no AN is generated by the LU. Instead, all transmit power is allocated to correct message transmission, while $\boldsymbol{p}$ and $\boldsymbol{q}$ are optimized according to (17), by setting $\alpha=1$. The proposed scheme performs similarly to the benchmark at low SNR, where the eavesdropper's detection ability is limited. However, it significantly outperforms the benchmark at high SNR values, where using a fraction of the transmit power to generate AN ensures outage at the eavesdropper, while using all available power to transmit the correct message allows the eavesdropper to decode the transmitted message. This can be seen in Fig. 4, which plots the optimal α for different values of β.

Fig. 3 shows the optimal access probability q of each user versus the transmit SNR, for different values of β. The low access probability at low SNR is expected because the system conditions cannot ensure reliable message transmission, and increasing the frequency with which the users access the channel is pointless. As the SNR increases, the access probability of the users also increases. Interestingly, however, in the proposed scheme, it decreases again in the $35-40$ dB range. This can be explained by considering Fig. 4. Specifically, at these SNRs, the optimal α changes to ensure outage at the eavesdropper, whereas before this was not necessary due to

This article has been accepted for publication in IEEE Wireless Communications Letters. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/LWC.2024.3468469

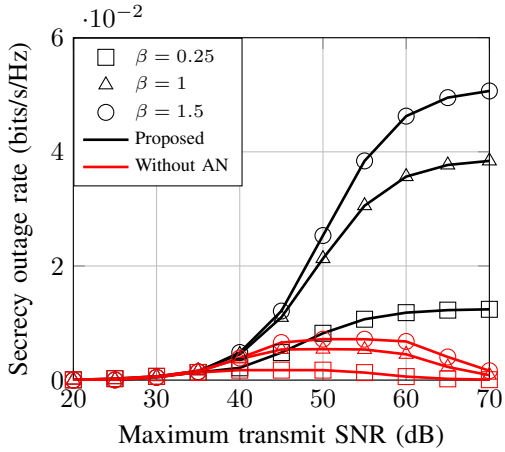

Fig. 2. System secrecy outage rate vs maximum transmit SNR.

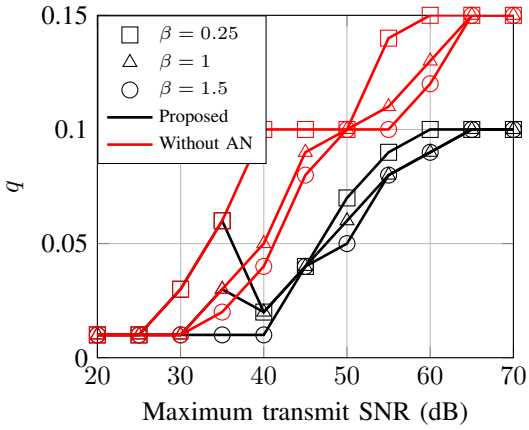

Fig. 3. Optimal access probability vs maximum transmit SNR.

the low received SNR at the eavesdropper. This results in less power being allocated to the correct message transmission, and thus a worse received SNR at the BS. To compensate for the degraded conditions, the optimal access probability decreases. From this point on, increasing the SNR, leads to higher access probability, until it reaches its maximum $1/N = 0.1$, which is the optimal access probability in the case of conventional slotted ALOHA. Further increasing the access probability results in a high collision rate and negatively affects the system performance.

Finally, in Fig. 4, it is also observed that for low SNR values, i.e., SNR < 35 dB, $\alpha = 1$ is preferred, while for SNR > 35 dB the system performs better with lower α. This can be explained by the fact that when the SNR is low enough, neither the BS nor the eavesdropper can reliably detect the transmitted message. Thus, using AN is detrimental to the system because there is no need to interfere with the eavesdropper's ability to decode, while all available power should be distributed to ensure that the message is received by the BS. On the other hand, at high SNR, the risk of the message being decoded by the eavesdropper becomes more critical than further increasing throughput. Therefore, the optimal α is one that ensures perfect secrecy, i.e., an outage at the eavesdropper will always occur. This result confirms Proposition 1, since the value of α saturates at $\frac{\beta}{\beta+1}$, and there is no reason to use a lower value.

V. Conclusions

In this paper, TS-ALOHA with randomly distributed LUs and eavesdroppers was proposed and investigated. The performance of a system, where the LUs allocate a percentage of the transmit power to AN, was evaluated through an appropriately defined metric called secrecy outage rate. Closed-form expressions for this metric were derived by calculating the outage probability at both the BS and the eavesdropper. The theoretical results were also validated by simulations, which explicitly showed how each parameter affects the system performance, and proved that the system performs better when AN is generated so that the eavesdropper's decoding capability is mitigated.

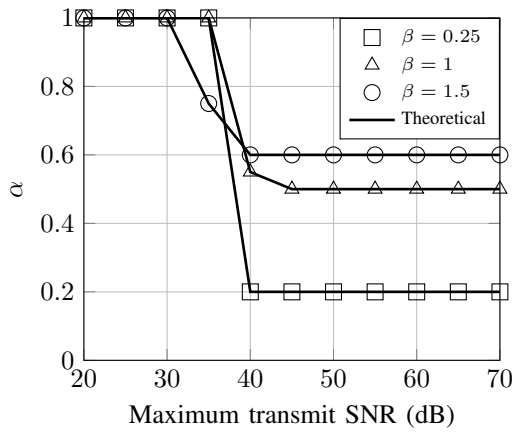

Fig. 4. Optimal fraction of power allocated to message transmission vs maximum transmit SNR.

References

[1] J. Karoliny, B. Etzlinger, R. Khanzadeh, A. Springer, and H.-P. Bernhard, "Network support layers trustworthiness computation for wireless networks," *IEEE Trans. Commun.*, pp. 1–1, 2024.

[2] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.

[3] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surv. Tut.*, vol. 16, no. 3, pp. 1550–1573, 2014.

[4] S. Zou, Y. Liang, L. Lai, and S. Shamai, "An information theoretic approach to secret sharing," *IEEE Trans. Inf. Theory*, vol. 61, no. 6, pp. 3121–3136, 2015.

[5] B. A. Bash, D. Goeckel, and D. Towsley, "Limits of reliable communication with low probability of detection on AWGN channels," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1921–1930, 2013.

[6] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, 2008.

[7] J. Choi, "Physical layer security for channel-aware random access with opportunistic jamming," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 11, pp. 2699–2711, 2017.

[8] H. Wei, X. Hou, Y. Zhu, and D. Wang, "Security analysis for Rayleigh fading channel by artificial noise," in *Proc. Sixth International Conference on Wireless Communications and Signal Processing (WCSP)*, pp. 1–6, 2014.

[9] G. Gomez, F. J. Martin-Vega, F. Javier Lopez-Martinez, Y. Liu, and M. Elkashlan, "Physical layer security in uplink NOMA multi-antenna systems with randomly distributed eavesdroppers," *IEEE Access*, vol. 7, pp. 70422–70435, 2019.

[10] A. A. Tegos, S. A. Tegos, D. Tyrovolas, P. D. Diamantoulakis, P. Sarigiannidis, and G. K. Karagiannidis, "Breaking orthogonality in uplink with randomly deployed sources," *IEEE Open J. Commun. Soc.*, vol. 5, pp. 566–582, 2024.

[11] I. S. Gradshteyn and I. M. Ryzhik, *Table of integrals, series, and products*. Academic press, 2014.

[12] S. A. Tegos, P. D. Diamantoulakis, A. S. Lioumpas, P. G. Sarigiannidis, and G. K. Karagiannidis, "Slotted ALOHA with NOMA for the next generation IoT," *IEEE Trans. Commun.*, vol. 68, no. 10, pp. 6289–6301, 2020.