electronics

MDPI

Article

Sensing and Secure NOMA-Assisted mMTC Wireless Networks

Urvashi Chaudhary [1], Mohammad Furqan Ali [1], Samikkannu Rajkumar [2] and Dushantha Nalin K. Jayakody [1,2,3,*]

[1] School of Computer Science and Robotics, National Research Tomsk Polytechnic University, 634034 Tomsk, Russia
[2] Centre for Telecommunication Research, School of Engineering, Sri Lanka Technological Campus, Padukka 10500, Sri Lanka
[3] Centro de Investigaçä em Tecnologias-Autónoma TechLab, Universidade Autónoma de Lisboa, 1169-023 Lisboa, Portugal
* Correspondence: djayakody@autonoma.pt

Abstract: Throughout this study, a novel network model for massive machine-type communications (mMTC) is proposed using a compressive sensing (CS) algorithm and a non-orthogonal multiple access (NOMA) scheme. Further, physical-layer security (PLS) is applied in this network to provide secure communication. We first assume that all the legitimate nodes operate in full-duplex mode; then, an artificial noise (AN) signal is emitted while receiving the signal from the head node to confuse eavesdroppers (Eve). A convex optimization tool is used to detect the active number of nodes in the proposed network using a sparsity-aware maximum a posteriori (S-MAP) detection algorithm. The sensing-aided secrecy sum rate of the proposed network is analyzed and compared with the sum rate of the network without sensing, and the closed-form expression of the secrecy outage probability of the proposed mMTC network is derived. Finally, our numerical results demonstrate the impact of an active sensing algorithm in the proposed mMTC network; improvement in the secrecy outage of the proposed network is achieved through increasing the distance of the Eve node.

Keywords: non-orthogonal multiple access; physical layer security; massive machine-type communications

Citation: Chaudhary, U.; Ali, M.F.; Rajkumar, S.; Jayakody, D.N.K. Sensing and Secure NOMA-Assisted mMTC Wireless Networks. *Electronics* **2023**, *12*, 2322. https://doi.org/10.3390/electronics12102322

Academic Editors: Zhi Lin, Xiaoyan Hu, Bin Li and Kang An

Received: 4 November 2022
Accepted: 2 December 2022
Published: 21 May 2023

1. Introduction

The perspective of fifth generation and beyond (5GB) networking technology, including the sixth generation (6G), is expected to fulfill the numerous shortcomings of existing wireless networks by providing mass connection of nodes simultaneously, enhancement of reliability, and reducing network unavailability [1]. Most significantly, 6G is anticipated to provide ultra-reliable communication, ultra-low latency, and wide accessibility. Recently, smart devices have enabled next-generation wireless networks to play an ample role in real-time data encryption/decryption, leading to further heavy data traffic flow. Therefore, the current wireless networks may not be completely supported by the available technologies. To cope with the related issues, the 6G wireless network is proposed with new spectrum and energy-efficient transmission techniques. However, multiple access scheme (MAS) collaborate in the development of large scale wireless networks [2]. Additionally, a potential MAS can be integrated as a non-orthogonal multiple access (NOMA) scheme. It is noteworthy that NOMA has been proposed for its high spectrum efficiency along with massive connectivity in 5G wireless networks. It serves the multiple connectivity of users within the same network with respect to time and frequency variation. At a glance, power-domain NOMA (PD-NOMA) is a subclass of NOMA schemes which allows users to convey their information using varying power levels and in superposition coding terminology. Similarly, the successive interference cancellation (SIC) technique is applied at the receiver end for decoding of signals in NOMA-based communications networks.

Indeed, power distribution scheduling enhances the performance of a full NOMA-based wireless network [3,4]. Moreover, the base station (BS) transmits all users' information through the same channel in a NOMA scenario. Further, the position of each user is identified by the effective channel gain in the queue. NOMA facilitates and assign a higher fraction of power to the users having weak signal strength [5]. Cooperative communication is an efficient way to enhance capacity while improving transmission reliability and spatial diversity. Users or dedicated relays cooperate among themselves to improve the transmission reliability of the system [6]. Further, to improve the spectrum efficiency and system throughput, the authors in [7] have investigated an amplify-and-forward (AF) relay-based NOMA network by implying Nakagami-m fading channels. Most recently, similar work has been proposed in [8], where the authors use a physical layer network coding (PLNC)-based NOMA wireless network to improve spectral and temporal efficiency.

Intermittent and sporadic user activity in wireless communication is a major characteristic of massive machine-type communications (mMTC) networks, known as machine-to-machine (M2M) communication. Originally, the concept of an mMTC was proposed by the International Telecommunications Union (ITU) to provide large-scale connectivity services through cellular networks for massive machine-type communications devices. As part of new radio technology, the deployment of NOMA in mMTC has attracted the attention of industrial communities [9]. Further, mMTC has been viewed as a promising technology for innovation with numerous smart sensors immersed in machine learning techniques and intelligence [10]. When an mMTC operates with a large number of devices, it mainly faces the issues of scalability, modeling, coverage, and congestion. Due to massive signaling overhead, NOMA schemes have been used to overcome such problems and improve massive access.

In an mMTC system, a limited number of users are expected to transmit short data packets to the Access Point (AP); in each time slot, a large number of user devices are registered to an AP [11]. To obtain massive access, an mMTC network is mainly focused on the uplink NOMA systems, in which a small number of active users can randomly transmit data at any time slot without any trembling process [12]. Therefore, the multiple distribution of active users inspires the formulation of the multi-user detection problem under the compressive sensing (CS) framework. The CS is a novel sampling paradigm used to reconstruct a sparse physical signal that samples signals in a much more efficient way than the established Nyquist sampling theorem [13]. As a result, the CS is a more suitable method for detecting the active nodes in a particular region of an mMTC wireless network.

In contrast, the field of physical layer security (PLS) has been introduced to achieve a secure communication platform, which implies critical issues over wireless networks in different scenarios [14]. The PLS was proposed by Wyner to improve the security of the network as an alternative approach to the cryptographic techniques [15]. The advantage of PLS is that it protects information by exploiting intrinsic characteristics of the communications medium, thereby promising wireless security [16]. In existing works, authors [17,18] have considered the PLS for NOMA-based networks for single-antenna and multiple-antenna networks under the stochastic geometry concept. PLS can be applicable considering the physical layer properties of the communication system, such as noise, interference, and the time-varying property of fading channels [19]. Recently, a NOMA-based uplink mMTC network model was developed in [20] and its performance was studied. The basic idea behind PLS is to reduce the the signal characteristics of the intended receiver for an eavesdropper (hereinafter referred to as Eve) [21]. Due to the broadcast nature of wireless networks, transmission between authorised users can easily be overheard by Eve for interception. It is challenging to deploy an active Eve or multiple Eves within heterogeneous networks [22]. A comprehensive review of PLS techniques for internet of things (IoTs) applications is discussed in [23], followed by a survey of existing PLS techniques and the characteristics of IoT.

1.1. Motivation

Motivated by the existing research, here we propose a novel mMTC network with a view to 6G networking system. As the existing research works have demonstrated that many network nodes are in idle condition, it is necessary to develop a low-power-consumption wireless network that can provide the high capacity needed for massive connectivity. Throughout this study, we propose a system model for massive connectivity within the 6G wireless networking approach. More specifically, we focus on constructing a suitable algorithm for sensing the active nodes in the given region of the mMTC networks, which can greatly improve overall network performance. In fact, mMTC is one of the major requirements of a 6G wireless network that can fulfill real-time data streaming applications in fields such as health care, industrial monitoring, traffic control, agriculture, etc. In another direction, providing secure communication in the mMTC networks, such as for command message passing in military contexts or control messages in industry, is another major concern. Therefore, in this a new network model for mMTC a network is proposed using PLS and CS algorithms to enhance sensing and secure communications.

1.2. Contributions

The main contributions of this paper can be summarized as follows:

- Throughout this study, we propose novel massive connectivity of machine-type communication system towards the 6G networking system utilizing the PLS.
- In an mMTC, the detection of inactive/active nodes is challenging; therefore, a new approach for detection is investigated in this study using the CS algorithm.
- Throughout this study, analytical expressions are provided and then verified by simulation results, and the end-to-end (E2E) performance metrics of the proposed system, such as secrecy and outage probability, are derived in detail.

The rest of the paper is organized as follows. In Section 2, the system model of the proposed network is discussed and the CS algorithm is explained. In Section 3, the performance aspects of the proposed mMTC network, such as the sensing-aided sum rate and secrecy outage probability, are explained. In Section 4, our numerical analysis is discussed, and lastly we provide concluding remarks in Section 5.

2. System Model

In the proposed system model, we consider an mMTC network in which $N+1$ number of nodes are distributed randomly in the given region, as in Figure 1. Among the $N+1$ nodes, only one node acts as a head node (the blue-colored node), and serves the remaining N nodes using a NOMA scheme. The geometrical model of the region is formulated as a circular region, and based on the distances of the nodes, a set of nodes is located in the inner circular region (near users) and the remaining nodes distributed in the outer circular region (far users). Because the number of nodes in a particular region is dynamic, it can be modeled as an homogeneous Poisson point process (HPPP) [24]. In this mMTC model, the radii of the inner and outer circular regions are denoted by n_r and f_r, respectively. In practical mMTC networks, there is a security issue that frequently arises due to unauthorized nodes, which are indicated as eavesdroppers (Eves) in this proposed model. An Eve node wants to trace confidential messages from the legitimate nodes. Hence, all nodes are designed in full-duplex mode, such that they always generate artificial noise (AN) while receiving message from the head node, which is intended to confuse any Eve nodes.

In existing mMTC networks, several of the nodes are in inactive condition due to certain practical issues. In such a scenario, random allocation of power to all users is not a favorable approach. Therefore, it is necessary to develop a suitable algorithm to sense all the active nodes in mMTC networks in order to enhance network performance. In this work, a single measurement vector-based CS algorithm [25] is used to sense active nodes.

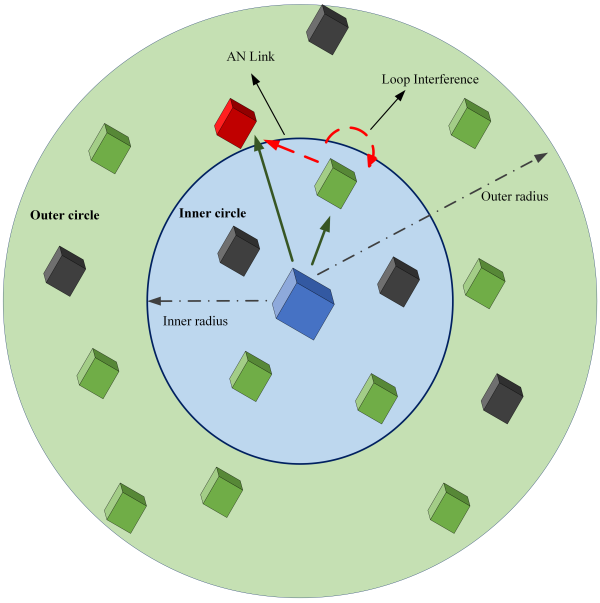


Figure 1. The proposed NOMA-assisted mMTC Wireless Networking System model, with active (green) and inactive (block) nodes distributed randomly in the circular region; an Eve node (red) tries to trace the confidential message information, and the blue node acts as the head node.

2.1. Active Nodes Sensing

We assume that each node in the mMTC network is active with a probability of $p_{act} << 1$ and that the head node identifies the activity of each node by simply checking whether or not a particular node has any useful information. Further, it is assumed that at any time only few nodes are active and that the head node receive the signals from both the active and inactive nodes; hence, the network can be modeled as a sparse vector. Thus, the CS algorithm represents a suitable method for detecting the sparse signals. The ith node ($i \in 1, \ldots, N$) transmits its message frame to the head node using binary phase shift keying (BPSK) modulation scheme, which is denoted as $\mathbf{x}_i$. Each frame consists of M BPSK symbols $\mathbf{x}_i = (\mathrm{s}_{i,1}, \ldots, \mathrm{s}_{i,M})$. Note that the proposed mMTC network is developed for low power and low data rate communications, such as e-healthcare, industrial automation, home automation, etc.; hence, BPSK modulation is sufficient to transmit control messages. The messages received from all N nodes can be represented as an $(\mathrm{NM} \times 1)$ sparse vector, as provided by $\mathbf{x} = (\mathbf{x}_1, \ldots, \mathbf{x}_N)^T$, where $\mathbf{x}_i = 0$ if the$i$th node is inactive. Therefore, the received signal at the head node is

$$\mathbf{y} = \mathbf{G}\mathbf{x} + \mathbf{z}, \tag{1}$$

where $\mathbf{G}$ is a measurement matrix $(\mathrm{N}' \times \mathrm{NM})$ designed using $(\mathrm{N}' \times \mathrm{NM})$ channel matrix $\mathbf{H}$ in which $\mathrm{N}' = \mathrm{qM} + \max_i(L_i - 1 + \tau_i)$, where L_i is the number of channel taps in the ith node, τ is the relative delay and $(\mathrm{NM} \times \mathrm{NM})$ spreading matrix $\mathbf{S}$ with spreading factor q [26] of the ith node, and z is additive white Gaussian noise (AWGN) with zero mean and variance σ^2. Using the sparsity-aware maximum a posteriori (S-MAP) detection algorithm [25], the active nodes are identified as follows:

$$\tilde{\mathbf{x}} = \min_{\mathbf{x}} \frac{1}{2} \|\mathbf{y} - \mathbf{G}\mathbf{x}\|_2^2 + \mu \|\mathbf{x}\|_1^1 \tag{2}$$

where $\mu = \ln \frac{1-p_{act}}{p_{act}/2}$, $p_{act} << 1$ is the active devices probability, $\tilde{\mathbf{x}}$ is the estimated sparse vector, and its sum of non-zero elements provides the total number of active nodes, which is denoted as N_{act}. By sensing the indices of the non-zero elements of the sparse vector, the head node allocates power to all the active nodes according to the NOMA scheme, thereby enhancing the performance of the mMTC network.

To improve active device detection in mMTC networks, it is necessary to analyze the active device detection error at the receiver. The normalized average mean square error ζ_{act} of active device detection can be calculated as follows:

$$\zeta_{act} = \frac{\sum_{c=1}^{\mathrm{M}^{'}} \|\mathbf{x} - \tilde{\mathbf{x}}\|_2^2}{\sum_{i=1}^{\mathrm{M}} \|\mathbf{x}\|_2^2}, \tag{3}$$

where $\mathrm{M}^{'}$ is the number of iterations. It is noteworthy that active device detection mainly depends on parameters such as the percentage of active devices κ, spreading factor q, and signal-to-noise ratio (SNR). In addition, the normalized average mean square error is helpful in analysing device detection via the S-MAP algorithm; device detection improvement can be achieved by increasing the SNR values, which is discussed in detail in Section 4.

2.2. Sensing-Aided Downlink Transmission

By applying the S-MAP algorithm, the head node is able to determine the status of the nodes. Thus, the head node allocates power only to active nodes based on the channel conditions. The channel gains are arranged in ascending order ($|h_1|^2 < |h_2|^2 < \cdots < |h_{N-1}|^2 < |h_N|^2$), and power allocation is performed correspondingly ($P_1 > P_2 > \cdots > P_{N-1} > P_N$). Note that an mMTC networks contains a large number of nodes; hence, allocating power after dividing the nodes into a number of groups is preferable, and is the approach considered in the rest of this work. Using the NOMA scheme, the head node superimposes all active node signals as $\mathbf{x} = \sum_{i=1}^{T} \alpha_i \sqrt{P_h} \mathbf{x}_i$, where P_t is the head node's transmitting power. Here, the power allocation coefficient α_i must satisfy the condition $\alpha_1 > \alpha_2, \ldots, \alpha_{N-1} > \alpha_N$ and $\alpha_1 + \alpha_2 + \cdots + \alpha_N = 1$.

For downlink transmission, the head node transmits the NOMA signal to all the nodes simultaneously. Because each node adopts full-duplex mode, it can emit the AN signal while receiving the signal from the head node. In addition, each node suffers from loop interference (LI) due to full-duplex operation. Here, let the ith node act as a near node, n and let the $i+1$th node act as a far node, f. Because the transmit signals are in the form of frames, and because each frame consists of M symbols, the kth $\in (1, \ldots, M)$ NOMA symbol can be written as $\mathrm{s}'_{\mathrm{k}} = \sum_{i=1}^{T} s_{\mathrm{i,k}}$. Therefore, the kth $\in (1, \ldots, M)$ received symbol at the near node n can be written as

$$y^k_{\mathrm{h,n}} = h_{\mathrm{h,n}} s'_{\mathrm{k}} + h_{\mathrm{LI}} s_{\mathrm{LI}} + z^k_{\mathrm{h,n}}, \tag{4}$$

where $h_{\mathrm{h,n}} = \frac{h'_{\mathrm{h,n}}}{1+d^{\alpha}_{\mathrm{h,n}}}$ is the channel coefficient between the head node and near node and subscript h denote the head node. Furthermore, a channel modeled using small- and large-scale fading and its channel gain follow the exponential distribution, with mean 0 and variance v_{n}. Additionally, the parameters are defined as the follows: the distance from the head node to the near node is $d_{\mathrm{h,n}}$, the path loss exponent is α, the channel coefficient of the LI is h_{LI}, which is exponentially distributed with mean 0 and variance v_{LI}, and the AWGN is $z^k_{\mathrm{n,k}}$, and is defined using $\mathcal{CN} \in (0, \sigma^2)$. The received signal from the far node can be calculated in a similar way.

At the same time, Eve traces the signal from the head node; the signal received from Eve can be expressed as

$$y^k_{\mathrm{h,e}} = h_{\mathrm{h,e}} s'_{\mathrm{k}} + h_{\mathrm{n,e}} s_{\mathrm{AN}} + z^k_{\mathrm{h,e}}, \tag{5}$$

where $h_{\mathrm{h,e}} = \frac{h'_{\mathrm{h,e}}}{1+d^{\alpha}_{\mathrm{h,e}}}$ is the channel coefficient between the head node and Eve and s_{AN} is the AN signal, which is generated using a pseudo-noise (PN) sequence. Its channel gain follows the exponential distribution, with mean 0 and variance v_{e}. However, here $d_{\mathrm{h,e}}$ is the distance from the head node to Eve, $h_{\mathrm{n,e}}$ is the channel coefficient between the near node and Eve, and $z^k_{\mathrm{h,e}}$ is the AWGN at Eve. Note that the AN signal is received from the far node with channel a coefficient of $h_{\mathrm{f,e}}$.

3. Coverage, Capacity, and Outage Analysis of Proposed mMTC

3.1. Uplink Coverage Probability of the mMTC

The proposed mMTC network is designed for short-distance communications; hence, the propagation model in the uplink is designed using a stretched exponential path loss (SEPL) model [27]. In this SEPL model, multipath fading is modeled by $\alpha - \mu$ distribution, where α is the average multiplicative attenuation, μ is the integer constant, and the transmit power attenuation is modeled as $e^{\alpha r^{\beta}}$, where r is the distance, r^{β} is the number of obstructions in the path, and β is the model parameter. Further, the maximum power needed at a distance $r_m = ln^{\frac{1}{beta}} \frac{P_m}{P_o}^{\frac{1}{\alpha}}$ to avoid outage of an mMTC node is P_m. Therefore, the cumulative distribution function (CDF) of this channel is modeled by

$$F_X(x) = \frac{\gamma(\mu, \mu x^{\alpha/2})}{\Gamma(\mu)}, \tag{6}$$

where $\Gamma(.)$ is the Gamma function and $\gamma(.,.)$ is the lower incomplete gamma function. The signal-to-interference plus noise (SINR) of the ith mMTC device at the base station (BS) is expressed as

$$\gamma_{UL}^{i} = \frac{P_i h_i}{\sum_{n=1, n\neq i}^{N} P_n h_n e^{\alpha r_n{}^{\beta}} + \sigma^2}, \tag{7}$$

The uplink coverage probability of the proposed mMTC network is provided by

$$P_C = 1 - \mathbb{E}\left[\frac{\gamma(\mu, \mu x^{\alpha/2})}{\Gamma(\mu)}\right], \tag{8}$$

In contrast, using $\gamma(\mu, v) = (\mu - 1)![1 - e^{-v} e_{\mu-1}(v)]$ and $\Gamma(\mu) = (\mu - 1)!$ it can be simplified as

$$P_C = 1 - \mathbb{E}\left[\frac{(\mu - 1)![1 - e^{-v} e_{\mu-1}(v)]}{(\mu - 1)!}\right], \tag{9}$$

Further, (9) can be simplified to obtain (10):

$$P_C = \mathbb{E}\left[e^{-v} e_{\mu-1}(v)\right], \tag{10}$$

where $v = \left[\frac{(2^R - 1)(\sum_{n=1, n\neq i}^{N} P_n h_n e^{\alpha r_n{}^{\beta}})}{P_i}\right]^{\alpha/2}$ and $e_{\mu}(x) = 1 + x + x^2/2! + \ldots + x^{\mu}/\mu!$ Here, let $\alpha = 2$ and $\mu = 1$; then, the coverage probability of the proposed mMTC network can be simplified as follows:

$$P_C = \mathbb{E}\left[e^{-(\frac{(2^R - 1)}{P_o})(\sum_{n=1, n\neq i}^{N} P_n h_n e^{\alpha r_n{}^{\beta}} + \sigma^2)}\right], \tag{11}$$

Expression (11) is a complex equation; therefore, by splitting the exponential term into two parts it becomes

$$P_C = e^{-\frac{2^R - 1}{SNR}} \mathbb{E}\left(e^{-\frac{2^R - 1}{P_o}(\sum_{n=1, n\neq i}^{N} P_n h_n e^{\alpha r_n{}^{\beta}})}\right), \tag{12}$$

By taking $s = (2^R - 1)/P_o$, the coverage probability expression can be simplified using the Laplace transform; thus, P_C can be written as

$$P_C = e^{-\frac{2^R - 1}{SNR}} \mathbb{L}_I(s), \tag{13}$$

where $\mathbb{L}_I(s)$ is the Laplace transform of the interference term. For further integration, (13) can be written as follows:

$$\mathbb{L}_I(s) = \mathbb{E}(e^{-s\sum_{n=1,n\neq i}^{N} P_n h_n e^{\alpha r_n{}^{\beta}} \mathbb{1}(P_n e^{\alpha r_n{}^{\beta}} < P_o)}), \tag{14}$$

By implying the exponential term, (14) can be modifies as follows:

$$\mathbb{L}_I(s) = \prod_{n=1,n\neq i}^{N} \mathbb{E}(e^{-sP_n h_n e^{\alpha r_n{}^{\beta}} \mathbb{1}(P_n e^{\alpha r_n{}^{\beta}} < P_o)}), \tag{15}$$

With the Laplace transformation $\mathbb{L}_I(s)$ using [28], the $\mathbb{L}_I(s)$ of the coverage probability can be simplified as follows:

$$\mathbb{L}_I(s) = e^{\left(\frac{-2\pi\rho_m\lambda_m}{N_R}\mathbb{E}\left(\int_{ln\,\frac{1}{beta}}^{\infty} \frac{P_m}{P_o}^{\frac{1}{\alpha}} (1-e^{-sP_n h_n e^{\alpha r_n{}^{\beta}}}) r_n dr_n\right)\right)}, \tag{16}$$

where ρ_m is the active device probability, λ_m is the increasing density of active devices, and N_R is the number of resource blocks. By applying the Laplace transform to $e^{-sP_n h_n e^{\alpha r_n{}^{\beta}}}$, we obtain the expression in exponential form, as follows:

$$\mathbb{L}_I(s) = e^{\left(\frac{-2\pi\rho_m\lambda_m}{N_R}\mathbb{E}\left(\int_{ln\,\frac{1}{beta}}^{\infty} \frac{P_m}{P_o}^{\frac{1}{\alpha}} (1-\frac{1}{1+sP_n e^{\alpha r_n{}^{\beta}}}) r_n dr_n\right)\right)}, \tag{17}$$

Let $y = sP_n e^{\alpha r_n{}^{\beta}}$ and $\mathbb{L}_I(s)$ be the coverage probability, which is integrated as follows:

$$\mathbb{L}_I(s) = e^{\left(\frac{-2\pi\rho_m\lambda_m}{\beta\alpha^{2/\beta}N_R}\mathbb{E}\left(\int_0^{sP_o} \frac{ln(\frac{sP_o}{y})^{(\frac{2}{\beta}-1)}}{y+1} dy\right)\right)}, \tag{18}$$

Setting $s = (2^R - 1)/P_o$ and $\beta = 2$, the coverage probability of the proposed mMTC networks is determined as follows:

$$P_C = e^{-\frac{(2^R-1)}{SNR}} e^{\left(\frac{-2\pi\rho_m\lambda_m}{\beta\alpha^{2/\beta}N_R} ln(2^R)\right)}, \tag{19}$$

3.2. Sensing-Aided Sum Rate

Because there are N nodes and each node transmits M symbols, the total number of symbols is MN. In the downlink, each node receives a NOMA signal, which consist of MN symbols, and decodes it on a symbol-by-symbol basis using an SIC operation. In downlink NOMA, the near node applies SIC and the far node directly decodes its message while treating the near node message as interference. The near node first decodes the far node's message, then it removes the decoded far node message after decoding its own message. The signal-to-interference plus noise ratio (SINR) of a far node, f for decoding a near node, n in the presence of LI can be written as

$$\Gamma_{\mathrm{f}\to\mathrm{n}} = \frac{|h_{\mathrm{h,n}}|^2 \alpha_f P_h}{\sigma^2 + |h_{\mathrm{h,n}}|^2 \sum_{q=1}^{q<f} \alpha_q P_{\mathrm{h}} + |h_{\mathrm{LI}}|^2 P_{\mathrm{LI}}}, \tag{20}$$

where $P_{LI} = \sum_{q=1}^{q=N} \alpha_q P_h$ is the LI power. For the case of two nodes, this can be further simplified as

$$\Gamma_{\mathrm{f}\to\mathrm{n}} = \frac{|h_{\mathrm{h,n}}|^2 \alpha_f P_h}{\sigma^2 + |h_{\mathrm{h,n}}|^2 \alpha_n P_h + |h_{\mathrm{LI}}|^2 P_{LI}}. \tag{21}$$

After omitting the far node message, the near node decodes its own message as follows:

$$\Gamma_{\mathrm{n}} = \frac{|h_{\mathrm{h,n}}|^2 \alpha_n P_h}{\sigma^2 + |h_{\mathrm{LI}}|^2 P_{\mathrm{LI}}}. \tag{22}$$

Similarly, the SINR of the far node can be written as

$$\Gamma_{\mathrm{f}} = \frac{|h_{\mathrm{h,f}}|^2 \alpha_f P_h}{\sigma^2 + |h_{\mathrm{h,f}}|^2 \alpha_n P_h + |h_{\mathrm{LI}}|^2 P_{\mathrm{LI}}}. \tag{23}$$

Eve receive NOMA messages from the legitimate nodes as well; therefore, the SINR of the Eve node can be written as

$$\Gamma_{\mathrm{n,e}} = \frac{|h_{\mathrm{h,e}}|^2 \alpha_n P_h}{\sigma^2 + |h_{\mathrm{n,e}}|^2 P_{\mathrm{AN}}}, \tag{24}$$

$$\Gamma_{\mathrm{f,e}} = \frac{|h_{\mathrm{h,e}}|^2 \alpha_f P_h}{\sigma^2 + |h_{\mathrm{h,e}}|^2 \alpha_n P_h + |h_{\mathrm{f,e}}|^2 P_{\mathrm{AN}}}. \tag{25}$$

Using the above SINR expressions, the secrecy sum rate of the proposed mMTC network can be calculated. The secrecy rate of the near node can be expressed as

$$C_{s,n} = [\mathrm{C_n} - \mathrm{C_{e,n}}]^+; \; C_{s,f} = [\mathrm{C_f} - \mathrm{C_{e,f}}]^+, \tag{26}$$

where $[a]^+$ indicates the $max(0, a)$, $\mathrm{C_n}$ and C_{f} are the near node and far node capacities, respectively, and $C_{\mathrm{e,\,n}}$ and $C_{\mathrm{e,\,f}}$ are the near Eve node and far Eve node capacities, respectively. The mathematical expressions for the the secrecy rates $\mathrm{C_n}$ and C_{f} are provided by

$$\mathrm{C_n} = log\left(1 + \frac{|h_{\mathrm{h,n}}|^2 \alpha_n P_h}{\sigma^2 + |h_{\mathrm{LI}}|^2 P_{\mathrm{LI}}}\right), \tag{27}$$

$$C_{\mathrm{f}} = log\left(1 + \frac{|h_{\mathrm{h,f}}|^2 \alpha_f P_h}{\sigma^2 + |h_{\mathrm{h,f}}|^2 \alpha_n P_h + |h_{\mathrm{LI}}|^2 P_{\mathrm{LI}}}\right), \tag{28}$$

Similarly, the rates of the $\mathrm{C_{n,e}}$ and $C_{\mathrm{f,e}}$ are written as

$$\mathrm{C_{n,e}} = log\left(1 + \frac{|h_{\mathrm{h,e}}|^2 \alpha_n P_h}{\sigma^2 + |h_{\mathrm{n,e}}|^2 P_{\mathrm{AN}}}\right). \tag{29}$$

$$C_{\mathrm{f,e}} = log\left(1 + \frac{|h_{\mathrm{h,e}}|^2 \alpha_f P_h}{\sigma^2 + |h_{\mathrm{h,e}}|^2 \alpha_n P_h + |h_{\mathrm{f,e}}|^2 P_{\mathrm{AN}}}\right). \tag{30}$$

Without sensing the active nodes, the total transmit power P_{h} of the head node is shared among N legitimate nodes using the NOMA scheme P_{h}/N. Thus, the performance of the mMTC network falls due to power being allocated to inactive nodes. However, when using the sensing algorithm, the head node shares power only among active nodes P_{h}/T, which significantly improves the secrecy sum rate of the proposed mMTC network.

Finally, the secrecy sum rate of the proposed NOMA-based mMTC network can be expressed as

$$C_{mtc} = \sum_{q=1}^{q=T} \mathrm{C_{s,q}}. \tag{31}$$

3.3. Secrecy Outage Probability

In this section, the secrecy outage probability of the near node is discussed. However, it is easy to extend this analysis to the far node secrecy outage. The secrecy outage probability of the near node can be written as

$$P_{\text{s,out}}(R) = Pr([\text{C}_\text{n} - \text{C}_\text{n,e}] < R), \tag{32}$$

where R is the threshold data rate. Substituting C_n and $\text{C}_\text{n,e}$, the secrecy outage becomes

$$P_{\text{s,out}}(R) = Pr\left(log\frac{1+\Gamma_\text{n}}{1+\Gamma_\text{n,e}} < R\right), \tag{33}$$

By rearranging (18), the secrecy outage probability of the near node is

$$P_{\text{s,out}}(R) = \int_0^\infty Pr\Big(\Gamma_\text{n} < 2^R(1+\Gamma_\text{n,e}) - 1\Big) f_Y(y)dy, \tag{34}$$

Here, Γ_n and $\Gamma_\text{n,e}$ can be modelled as random variables X and Y, allowing the secrecy outage to be simplified as follows:

$$P_{\text{s,out}}(R) = \int_0^\infty \int_{-\infty}^{2^R(1+y)-1} f_X(x) f_Y(y)dxdy, \tag{35}$$

where $f_X(x)$ and $f_Y(y)$ denote the probability density function (PDF) of Γ_n and $\Gamma_\text{e,n}$, respectively. After integration and simplification, the secrecy outage probability of the near node can determined as

$$\begin{aligned} P_{\text{s,out}}(R) = {} & \frac{\pi}{2N}\sum_{i=1}^{N}\Psi_i - \frac{\pi}{2N}\sum_{i=1}^{N}\frac{\Psi_i l_{ne}\chi_i^2\alpha_i^2}{l_\text{h,e}\psi_i R_{th}}\exp\left(-\frac{\psi_i(R_{th}-1)}{\alpha_i SNR}\right)\sum_{k=1}^{K}\frac{\beta_i}{(x_k+\eta_1)^2+(x_k+\eta_2)} \\ & - \frac{\pi}{2N}\sum_{i=1}^{N}\frac{\Psi_i l_\text{n,e} l_\text{h,e}\alpha_i}{INR[\kappa l_\text{h.e} - \alpha_i l_\text{n,e}\psi_i R_{th}]}[(-\exp(\eta_1))\text{Ei}(-\eta_1) + \exp(\eta_2)\text{Ei}(-\eta_2)], \end{aligned} \tag{36}$$

where Ei(.) is the exponential integral function, $\kappa = (v_{LI}\psi_i R_{th} - \alpha_i - \psi_i v_{LI})$, $\chi_i = \frac{SNR\times l_\text{h,e} + INR\times\psi i R_{th}}{\alpha_i SNR\times INR}$, $\eta_1 = \frac{\alpha_i l_\text{n,e}}{l_\text{h,e}}\Gamma_i$, $\eta_2 = \frac{\psi_i R_{th}+\alpha_i-\psi_i}{\psi_i R_{th}}\Gamma_i$, $\beta_i = \frac{(K!)^2}{[L_i'(x_i)]^2 x_i}$, $L_K(x) = e^x\frac{d^k}{dx^K}(x^K e^{-x})$ and x_i is the zero point of $L_K(x)$.

Proof. See Appendix A. □

3.4. Outage Probability without Eve

Without Eve, the outage probability of the far node can be expressed as

$$P_\text{out}^\text{far}(R) = Pr\left(\frac{|h_\text{h,f}|^2\alpha_f P_h}{\sigma^2 + |h_\text{h,f}|^2\alpha_n P_h} < R\right). \tag{37}$$

Let $\omega_1 = \frac{\alpha_f P_h}{\sigma^2}$, $\omega_2 = \frac{\alpha_n P_h}{\sigma^2}$, then the outage probability of the far node can be simplified as [8].

$$P_\text{out}^\text{far}(R) = Pr\Big(|h_\text{h,f}|^2(\omega_1 - \omega_1\gamma_{th}) < R_{th}\Big), \tag{38}$$

Let $|h_\text{h,f}|^2 = x$; then, it becomes

$$P_\text{out}^\text{far}(R) = \int_{-\infty}^{\frac{R_{th}}{\omega_1-\omega_1 R_{th}}} f_X(x)dx, \tag{39}$$

Because x follows an exponential distribution, the outage probability of the far node without Eve can be determined as follows:

$$P_{\text{out}}^{\text{far}}(R) = 1 - e^{-\frac{R_{th}}{v(\omega_1 - \omega_1 R_{th})}}. \quad (40)$$

4. Results and Discussion

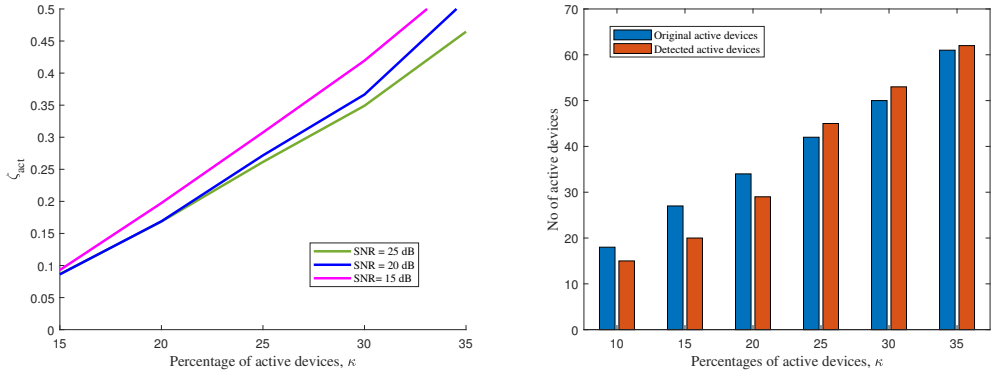
In this section, the secrecy sum rate and secrecy outage probability of the proposed NOMA-based mMTC network is discussed. In addition, active node detection in the mMTC network using the CS algorithm is described, as well as the use of the convex optimization toolbox '*cvx*' to estimate the sparsity of active nodes. Matlab software was used for all the simulations of performance metrics, including the coverage probability, sum rate, outage probability, and secrecy outage probability of the proposed mMTC network, and the legitimate node channel variance was fixed to 1 for all the simulations. The detailed simulation parameters are listed in Table 1.

Table 1. Simulation parameters used to obtain the expected results of the proposed mMTC system model.

S. No.	Parameters	Symbols	Value
1.	Radius of the inner circle	n_r	4 m
2.	Power allocation coefficient	α_i	0.7
3.	Path loss exponent	α	2
4.	Distance of the near node to Eve	$d_{\text{n,e}}$	3 m
5.	Data rate	R	1 b/s/Hz
6.	LI power	P_{LI}	-10 dBW
7.	AN power	P_{AN}	-10 dBW

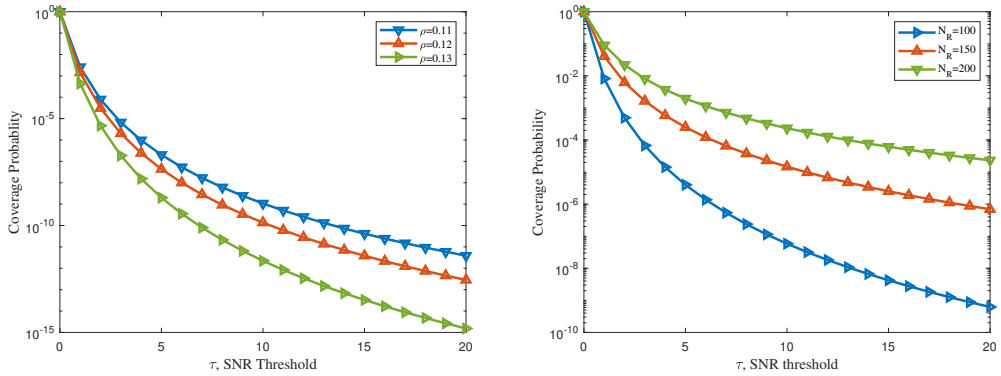
The normalized average mean square error of active device detection is shown in Figure 2a. A convex optimization tool is used to detect the active devices in the proposed mMTC network; the active devices are then modeled as a sparse vector. From this figure, it can be observed that the mean square error of active device detection increases when the percentage of active devices increases. Further, the performance of active device detection improves when the SNR values increase. Figure 2b shows the comparison of the total number of active devices detected in the proposed mMTC wireless networks. In this figure, it can be noted that even though the average mean square error increases with the percentage of active devices, the total number of active devices detected increases as well.

Figure 3a shows the uplink coverage probability of the proposed mMTC wireless network. In this simulation, the following parameters are considered: active device probability ρ is varied as 0.12, 0.13, and 0.14, SNR = -130 dBW, noise variance = -151.45 dBW, data rate R = 2 b/s/Hz, $\beta = 1/3$, increasing density of active devices $\lambda_m = 500$, number of resource blocks $N_R = 100$, path loss model parameter $\alpha = 1.1$. From this figure, it can be observed that the coverage probability of the proposed networked is reduced when increasing the active device probability. Therefore, better coverage of the proposed mMTC network can be achieved by increasing the active device probability. Similarly, the coverage probability of the proposed mMTC network is analyzed for various N_R values. In this figure, coverage of the proposed network is improved when increasing the number of resource blocks.



(**a**) (**b**)

Figure 2. (**a**) Normalized average mean square error of active device detection and (**b**) active device detection of the proposed mMTC network.



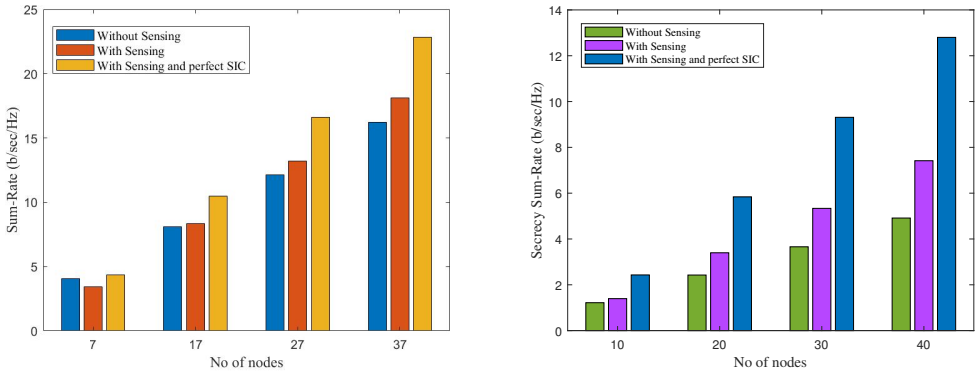
(**a**) (**b**)

Figure 3. (**a**) Uplink coverage probability of the proposed mMTC network for various ρ values and (**b**) uplink coverage probability of the proposed mMTC network for various N_R values.

Figure 4a shows the sum rate of the proposed NOMA-based mMTC network without Eve. In this simulation, the number of legitimate nodes is 40 and the LI power is -10 dBW. Active node detection is performed using the convex optimization toolbox. The sum rate of the proposed network is compared with the sensing-aided sum rate and perfect SIC-based sum rate. It can be observed that the active sensing algorithm is not effective when the number of nodes is low. However, the proposed mMTC network achieves significant improvement thanks to the active sensing algorithm as the number of nodes increases. Furthermore, it can be observed that, with perfect SIC and the active sensing approach, the sum rate of the proposed network is even better than the sum rate with sensing. Therefore, it can be concluded that the active node detecting approach plays a vital role in the mMTC network, enhancing overall network performance.

The secrecy sum rate of the proposed NOMA-based mMTC network is shown in Figure 4b. The number of legitimate nodes is 40, and AN and LI power are considered as -10 dBW. The secrecy sum rate is estimated by taking the sum rate difference between legitimate nodes and Eve nodes. The sum rate is compared with and without the sensing algorithm and perfect SIC. From this figure, it can be noted that the active sensing algorithm is effective in the proposed mMTC network even with a lower number of nodes. Furthermore, the sum rate is significantly increased when the number of nodes in the proposed network increases. However, with the presence of Eve, the sum rate of the proposed mMTC network is low compared to the network without Eve. For instance, with 30 nodes the secrecy sum rate with sensing is around 5 b/s/Hz, whereas without Eve the sum rate is 13 b/s/Hz. This makes the effect of the Eve node in the mMTC network very evident;

hence, designers ought to change the configuration of the network to obtain high quality of service even when Eve nodes ar present.

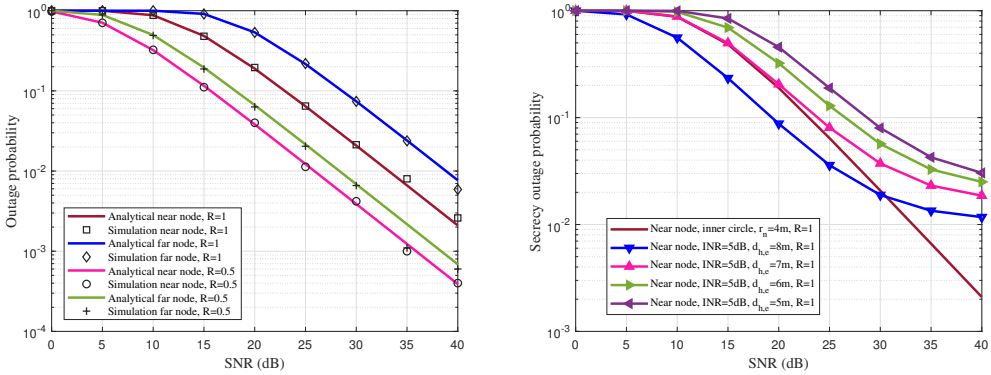


(**a**) (**b**)

Figure 4. (**a**) Sum rate of the proposed NOMA-based mMTC network without Eve and (**b**) secrecy sum rate of the proposed NOMA-based mMTC network with Eve.

Figure 5a shows the outage probability of the proposed mMTC network. In this simulation, the presence of Eve is omitted; hence, LI and AN power are not considered, and other parameters, such as the distance of the far node $d_{h,f}$ = 6 m, distance of the near node $d_{h,n}$ = 4 m, and path loss exponent $\gamma =$ 2 are used. The analytical results are validated using the presented simulation results. The outage probability of the far node and near node are compared using the rates R = 1 b/s/Hz and R = 0.5 b/s/Hz. At the target outage level of 10^{-2}, the near node needs 25 dBW SNR, whereas far node requires 28 dBW SNR. For a threshold data rate of R = 0.5 b/s/Hz, this indicates that an additional 3 dBW SNR is needed for the far node.

The secrecy outage performance of the proposed mMTC network is shown in Figure 5b. In this simulation, the following parameters are used: distance of the near node $d_{h,n}$ = 2 m, distance from near node to Eve node $d_{n,e}$ = 3 m, Gauss–Lagurre Quadrature K = 10, path loss exponent $\gamma = 2$, threshold data rate R = 1 b/s/Hz, and LI and AN power -10 dBW. From this figure, it can be observed that the outage performance of the proposed mMTC network is degraded due to the presence of LI and AN power. When the Eve node is near the head node, it receives a strong signal from the head node, degrading the network's outage performance. Therefore, it is better to always keep Eve nodes a certain distance away from the head node to ensure better network performance.



(**a**) (**b**)

Figure 5. (**a**) Outage probability of downlink NOMA-based mMTC network and (**b**) secrecy outage probability of downlink NOMA-based mMTC network.

5. Conclusions

In this study, a novel network model for an mMTC network is proposed using a NOMA scheme and the CS algorithm. Additionally, the PLS scheme is applied in this network to provide secure communication. Active node detection is performed in the proposed network using the S-MAP algorithm to improve the secrecy sum rate. Using the Laplace' transform, the mathematical expression for the coverage probability of the proposed network is derived, along with a closed-form expression of the secrecy outage probability of the proposed mMTC network. Finally, our numerical results demonstrate that the active device sensing algorithm plays a vital role in the proposed mMTC network by enhancing the efficient utilization of resources. Finally, the secrecy outage performance ensures secure communication while maintaining the QoS of the active nodes in the network.

Author Contributions: Conceptualization, U.C., S.R.; methodology, U.C, S.R., M.F.A.; validation, U.C., S.R., M.F.A.; formal analysis, U.C., S.R., D.N.K.J.; writing—original draft preparation, U.C., S.R., M.F.A.; writing—review and editing, S.R., M.F.A., D.N.K.J.; visualization, D.N.K.J.; funding acquisition, D.N.K.J. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the Cooperativa de Ensino Universitário (CEU), Portugal.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: This study did not report any data.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this study:

5Gb	Fifth Generation and beyond
6G	Sixth Generation
AN	Artificial Noise
AWGN	Additive White Gaussian Noise
BPSK	Binary Phase-Shift Keying
BS	Base Station
CDF	Cumulative Distribution Function
CS	Compressive Sensing
Eve	Eavesdropper
E2E	End-to-End
HPPP	Homogeneous Poisson Point Process
ITU	International Telecommunications Union
LI	Loop Interference
mMTC	massive Machine-Type Communications
M2M	Machine-to-Machine Communication
NOMA	Non-Orthogonal Multiple Access
PDF	Probability Density Function
PN	Pseudo-Noise
PLNC	Physical Layer Network Coding
PLS	Physical Layer Security
RB	Resource Block
S-MAP	Sparsity-aware Maximum A Posteriori
SELP	Stretched Exponential Path Loss
SC	Superposition Coding
SIC	Successive Interference Cancellation
SINR	Signal-to-Interference plus Noise Ratio
SNR	Signal-to-Noise Ratio

Appendix A

Because the sets of nodes are distributed randomly in the inner circular region, which can be modeled using HPPP, in (20) we can write $\int_{-\infty}^{2^R-1} f_X(x)dx$ as

$$\int_{-\infty}^{2^R-1} f_X(x)dx = Pr(\frac{|h_{\mathrm{h,n}}|^2\alpha_n P_h}{\sigma^2 + |h_{\mathrm{LI}}|^2 P_{\mathrm{LI}}} < R_{th}), \tag{A1}$$

where $R_{th} = 2^R - 1$ is the threshold SNR. Let $x = |h_{\mathrm{h,n}}|^2$, $y_1 = |h_{\mathrm{LI}}|^2$; then, (A1) can be written as

$$F_X(x) = \int_0^\infty Pr\left(x < \frac{R_{th}(y_1 P_{LI} + \sigma^2)}{\alpha_n P_h}\right) \times f_{Y_1}(y_1)dy_1. \tag{A2}$$

Inside the inner circular regions, all node distances are random in nature; thus, $d_{\mathrm{h,n}} = \mathrm{y}_2$ and its PDF can be written as

$$f_{Y_2}(y_2) = \frac{1}{\pi n_r^2}, \tag{A3}$$

The cumulative distributive function (CDF) of x can be written as follows [25]:

$$F_X(x) = \oint (1 - e^{(1+y_2^\alpha)x}) f_{Y_2}(y_2)dy_2. \tag{A4}$$

By applying limits, this can be modified as follows:

$$F_X(x) = \frac{2}{n_r^2} \int_0^{n_r} (1 - e^{(1+y_2^\alpha)x}) f_{Y_2}(y_2)dy_2. \tag{A5}$$

Using Gauss–Chebyshev quadrature [29], this can be further simplified as

$$F_X(x) \approx \frac{\pi}{2N} \sum_{i=1}^{N} \sqrt{(1-\eta_i^2)}(\eta_i + 1)(1 - e^{(1+\psi_i)x}), \tag{A6}$$

where $\eta_i = cos(\frac{2i-1}{2N}\pi)$ and $\psi_i = 1 + (\frac{n_r}{2}(\eta_i + 1))^\alpha$. By substituting (A6) and $f_{Y_1}(y_1)$ in (A2), the outage probability of the near user can be computed as

$$F_X(x) \approx \frac{\pi}{2N} \sum_{i=1}^{N} \Psi_i (1 - \frac{\alpha_i}{\alpha_i + v_{LI}\psi_i x} e^{-\frac{\psi_i R_{th}}{\alpha_i SNR}}),$$

where $SNR = \frac{P_h}{\sigma^2}$ is the signal-to-noise ratio (SNR) of the head node. Recall that the secrecy outage probability of the near node is

$$P_{\mathrm{s,out}}(R) = \int_0^\infty F_X(2^R(1+y) - 1) f_Y(y)dy, \tag{A7}$$

where $f_Y(y)$ is the PDF of Eve's SINR and $\Gamma_{\mathrm{n,e}}$, and can be determined as follows. First, compute the CDF of Eve; then, the PDF can be computed using the corresponding CDF. The CDF of $\Gamma_{\mathrm{e,n}}$ can be expressed as

$$F_Y(y) = Pr\left(\frac{|h_{\mathrm{h,e}}|^2\alpha_n P_h}{\sigma^2 + |h_{\mathrm{n,e}}|^2 P_{\mathrm{AN}}} < R_{th}\right). \tag{A8}$$

Note that $\alpha_n = \alpha_i$. Let $y = |h_{\mathrm{h,e}}|^2$, $y_3 = |h_{\mathrm{n,e}}|^2$; then, the above can be rewritten as

$$F_Y(y) = \int_0^\infty Pr\left(y < \frac{R_{th}(y_3 P_{AN} + \sigma^2)}{\alpha_i P_h}\right) f_{Y_3}(y_3)dy_3, \tag{A9}$$

Moreover, (A9) can be written in PDF form as

$$F_{\mathrm{Y}}(y) = \int_0^{\infty} \int_{-\infty}^{R_{th2}} f_Y(y) f_{Y_3}(y_3) dy dy_3, \tag{A10}$$

where $R_{th2} = \frac{R_{th}(y_3 P_{AN} + \sigma^2)}{\alpha_i P_h}$. After integrating and simplifying, the CDF of the Eve's SINR $\Gamma_{\mathrm{n,e}}$ can be computed as follows:

$$F_Y(y) = 1 - \frac{\alpha_i l_{e,n}}{\alpha_i l_{\mathrm{n,e}} + R_{th} l_{\mathrm{h,e}}} e^{-\frac{R_{th} l_{\mathrm{h,e}}}{\alpha_i \times INR}}, \tag{A11}$$

where $INR = \frac{P_{LI}}{\sigma^2}$ is the interference-to-noise ratio (INR) of the legitimate node. By integrating (A12), the PDF of $\Gamma_{\mathrm{n,e}}$ can be determined as follows:

$$f_Y(y) = \left(\frac{\alpha_i l_{\mathrm{n,e}} l_{\mathrm{h,e}}}{(\alpha_i l_{\mathrm{n,e}} + y l_{\mathrm{h,e}})^2} + \frac{l_{\mathrm{n,e}} l_{\mathrm{h,e}}}{INR(\alpha_i l_{\mathrm{n,e}} + y l_{\mathrm{h,e}})} \right) \exp(-\frac{y l_{\mathrm{h,e}}}{\alpha_i INR}), \tag{A12}$$

where $l_{\mathrm{n,e}} = 1 + d_{\mathrm{n,e}}^{\alpha}$, $l_{\mathrm{h,e}} = 1 + d_{\mathrm{h,e}}^{\alpha}$. By substituting (A7) and (A13) into (A8), the secrecy outage probability of the near node is determined as follows:

$$p_{\mathrm{s,out}}(R) = \frac{\pi}{2N} \sum_{i=1}^{N} \Psi_i \int_0^{\infty} (1 - \frac{\alpha_i}{\alpha_i + v_{\mathrm{LI}} \psi_i (2^R(1+y) - 1)} e^{-\frac{\phi_i (2^R(1+y)-1)}{\alpha_i SNR}}) \left(\frac{\alpha_i l_{\mathrm{n,e}} l_{\mathrm{h,e}}}{(\alpha_i l_{\mathrm{n,e}} + y l_{\mathrm{h,e}})^2} + \frac{l_{\mathrm{n,e}} l_{\mathrm{h,e}}}{INR(\alpha_i l_{\mathrm{n,e}} + y l_{\mathrm{h,e}})} \right) e^{-\frac{y l_{\mathrm{h,e}}}{\alpha_i INR}} dy. \tag{A13}$$

The above expression in (A13) consists of four terms; hence, the secrecy outage probability can be rewritten as

$$p_{\mathrm{s,out}}(R) = G(S_1 + S_2 + S_3 + S_4), \tag{A14}$$

where $G = \frac{\pi}{2N} \sum_{i=1}^{N} \Psi_i$. The parameters S_1, S_2, S_3, and S_4 are determined as follows:

$$S_1 = \int_0^{\infty} \frac{\alpha_i l_{\mathrm{n,e}} l_{\mathrm{h,e}}}{(\alpha_i l_{\mathrm{n,e}} + y l_{\mathrm{h,e}})^2} e^{-\frac{y l_{\mathrm{h,e}}}{\alpha_i INR}} dy, \tag{A15}$$

$$S_2 = \int_0^{\infty} \frac{l_{\mathrm{n,e}} l_{\mathrm{h,e}}}{INR(\alpha_i l_{\mathrm{n,e}} + y l_{\mathrm{h,e}})} e^{-\frac{y l_{\mathrm{h,e}}}{\alpha_i INR}} dy, \tag{A16}$$

$$S_3 = -\int_0^{\infty} \frac{\alpha_i}{INR(\alpha_i l_{\mathrm{n,e}} + y l_{\mathrm{h,e}}) + (\alpha_i + v_{LI} \psi_i R_{th3})} e^{-\frac{\psi_i R_{th3}}{\alpha_i SNR}} e^{-\frac{y l_{\mathrm{h,e}}}{\alpha_i INR}}, \tag{A17}$$

where $R_{th3} = (2^R(1+y) - 1)$.

$$S_4 = -\int_0^{\infty} \frac{\alpha_i^2}{(\alpha_i l_{\mathrm{n,e}} + y l_{\mathrm{h,e}})^2 + (\alpha_i + v_{LI} \psi_i R_{th3})} e^{-\frac{\psi_i R_{th3}}{\alpha_i SNR}} e^{-\frac{y l_{\mathrm{h,e}}}{\alpha_i INR}}. \tag{A18}$$

Using [30], (3.353.3), (3.352.4), and (3.352.4), the Gauss–Laguarre Quadrature, secrecy, and outage probability of the near user can obtained as in (25).

References

1. De Alwis, C.; Kalla, A.; Pham, Q.-V.; Kumar, P.; Dev, K.; Hwang, W.-J.; Liyanage, M. Survey on 6G frontiers: Trends, applications, requirements, technologies and future research. *IEEE Open J. Commun. Soc.* **2021**, *2*, 836–886. [CrossRef]
2. Hakeem, S.A.A.; Hussein, H.H.; Kim, H. Vision and research directions of 6G technologies and applications. *J. King Saud Univ. Comput. Inf. Sci.* **2022**, *34*, 2419–2442.
3. Melki, R.; Noura, H.N.; Chehab, A. Physical layer security for NOMA: Limitations, issues, and recommendations. *Ann. Telecommun.* **2021**, *76*, 375–397. [CrossRef]

4. Men, J.; Ge, J.; Zhang, C. Performance Analysis for Downlink Relaying Aided Non-Orthogonal Multiple Access Networks With Imperfect CSI Over Nakagami-*m* Fading. *IEEE Access* **2017**, *5*, 998–1004. [CrossRef]
5. Islam, S.M. R.; Avazov, N.; Dobre, O.A.; Kwak, K.-S. Power-domain non-orthogonal multiple access (NOMA) in 5G systems: Potentials and challenges. *IEEE Commun. Surv. Tut.* **2016**, *19*, 721–742. [CrossRef]
6. Ding, Z.;Peng, M.; Poor, H.V. Cooperative non-orthogonal multiple access in 5G systems. *IEEE Commun. Lett.* **2015**, *19*, 1462–1465. [CrossRef]
7. Men, J.; Ge, J.; Zhang, C. Performance analysis of nonorthogonal multiple access for relaying networks over Nakagami-*m* fading channels. *IEEE Trans. Veh. Technol.* **2016**, *66*, 1200–1208. [CrossRef]
8. Rajkumar, S.; Jayakody, D.N.K; Chang, Z.A. Hybrid NOMA-PLNC Wireless Relay Scheme. In Proceedings of the IEEE 18th Annual Consumer Commun & Networking Conference (CCNC), Las Vegas, NV, USA, 9–12 January 2021.
9. Arora, K.; Singh, J.; Randhawa, Y.S. A survey on channel coding techniques for 5G wireless networks. *Telecommun. Syst.* **2020**, *73*, 637–663. [CrossRef]
10. Mahmood, N.H.; Alves, H.; López, O.A.; Shehab, M.; Osorio, D.P.M.; Latva-Aho, M. Six Key Features of Machine Type Communication in 6G. In Proceedings of 2020 2nd 6G Wireless Summit (6G SUMMIT), Levi, Finland, 17–20 March 2020.
11. Yu, W. On the fundamental limits of massive connectivity. In Proceedings of 2017 Information Theory and Applications Workshop (ITA), San Diego, CA, USA, 12–17 February 2017.
12. Hong, J.-P.; Choi, W.; Rao, B.D. Sparsity controlled random multiple access with compressed sensing. *IEEE Trans. Wirel. Commun.* **2014**, *14*, 998–1010. [CrossRef]
13. Du, Y.; Dong, B.; Chen, Z.; Wang, X.; Liu, Z.; Gao, P.; Li, S. Efficient multi-user detection for uplink grant-free NOMA: Prior-information aided adaptive compressive sensing perspective. *IEEE J. Sel. Areas Commun.* **2017**, *35*, 2812–2828. [CrossRef]
14. ElHalawany, B.M.; Wu, K. Physical-Layer Security of NOMA Systems Under Untrusted Users. In Proceedings of 2018 IEEE Global Communications Conference GLOBECOM, Abu Dhabi, United Arab Emirates, 9–13 December 2018.
15. Wyner, A.D. The wire-tap channel. *Bell Syst. Tech. J.* **1975**, *54*, 1355-1387. [CrossRef]
16. Wang, D. Bai, B.; Zhao, W.; Han, Z. A survey of optimization approaches for wireless physical layer security. *IEEE Commun. Surv. Tutor.* **2018**, *21*, 1878–1911. [CrossRef]
17. Liu, Y.; Qin, Z.; Elkashlan, M.; Gao, Y.; Hanzo, L. Enhancing the Physical Layer Security of Non-Orthogonal Multiple Access-NOMA in Large-Scale Networks. *IEEE Trans. Wirel. Commun.* **2017**, *16*, 1656-1672. [CrossRef]
18. Rajkumar, S.; Jayakody, D.N.K.; Alkanhel, R.; Muthanna, A. Physical Layer Security in N-Pair NOMA-PLNC Wireless Networks. *IEEE Access* **2022**, *10*, 91356 – 91371. [CrossRef]
19. Furqan, H. M.; Hamamreh, J.; Arslan, H. Physical layer security for NOMA: Requirements, merits, challenges, and recommendations. *arXiv* **2019**, arXiv:1905.05064.
20. Han, S.; Xu, X.; Tao, X.; Zhang, P. Joint power and sub-channel allocation for secure transmission in NOMA-based MMTC networks. *IEEE Syst. J.* **2019**, *13*, 2476–2487. [CrossRef]
21. Singh, P.; Pawar, P.; Trivedi, A. Physical Layer Security Approaches in 5G Wireless Communication Networks. In Proceedings of 2018 FirstInternational Conference on Secure Cyber Computing and Communication (ICSCCC), Jalandhar, India, 15–17 December 2018.
22. Wang, W.; Teh, K.C.; Li, K.H.; Luo, S. On the impact of adaptive eavesdroppers in multi-antenna cellular networks. *IEEE Trans. Inf. Forensics Secur.* **2017**, *13*, 269–279. [CrossRef]
23. Sun, L.; Du, Q. A review of physical layer security techniques for Internet of Things: Challenges and solutions. *Entropy* **2018**, *20*, 730. [CrossRef]
24. Gong, C.; Yue, X.; Wang, X.; Dai, X. Enhancing Physical Layer Security With Artificial Noise in Large-Scale NOMA Networks. *IEEE Trans. Veh. Technol.* **2021**, *70*, 2349–2361. [CrossRef]
25. Alam, M.; Zhang, Q. A Survey: Nonorthogonal Multiple Access with Compressed Sensing Multiuser Detection for mMTC. *Wirel. Commun. Mob. Comput.* **2021**, *2021*, 8840519. [CrossRef]
26. Dekorsy, A.; Brueck, S. Is multiuser detection beneficial to mixed service UMTS networks? *Int. J. Electron. Commun.* **2005**, *59*, 473–482. [CrossRef]
27. Liu, Y.; Ding, Z.; Elkashlan, M.; Poor, H.V. Cooperative non-orthogonal multiple access with simultaneous wireless information and power transfer. *IEEE J. Sel. Areas Commun.* **2016**, *34*, 938–953. [CrossRef]
28. Kamel, M; Hamouda, W; Youssef, A. 'Uplink Coverage and Capacity Analysis of mMTC in Ultra-Dense Networks. *IEEE Trans. Veh. Technol.* **2020**, *69*, 746–759. [CrossRef]
29. Hildebrand, F.B. *Introduction to Numerical Analysis*; Dover: New York, NY, USA, 1987.
30. Gradshteyn, I.S; Ryzhik, I.M. *Table of Integrals, Series, and Products*, 6th ed.; Academic Press: New York, NY, USA, 2000.