

Non-Orthogonal Hash Access for Grant-Free IoT Blockchain Radio Access Networks

Jamil Farhat^{ID}, Jorge Felipe Grybosi^{ID}, *Graduate Student Member, IEEE*,
Glauber Brante^{ID}, *Senior Member, IEEE*, Richard Demo Souza^{ID}, *Senior Member, IEEE*,
and João Luiz Rebelatto^{ID}, *Senior Member, IEEE*

Abstract—We consider a blockchain radio access network where the devices share the wireless channel using the hash access (HA) protocol. In HA, devices obtain access to the channel with low collision probability and little control overhead upon reaching a valid hash value, below an advertised target. We elaborate on the HA protocol by proposing the non-orthogonal hash access (NOHA) scheme, where successive interference cancellation (SIC) is used with non-orthogonal multiple access (NOMA), dealing with collisions not handled by the standard HA protocol, boosting the network performance. Moreover, we find the optimal hash difficulty to access the channel that maximizes the network throughput. Analytical and numerical results show that with a single additional SIC iteration we are capable of achieving more than double the throughput of the standard HA protocol.

Index Terms—Blockchain, hash access, IoT, NOMA, SIC.

I. INTRODUCTION

THE EVOLUTION of wireless networks towards 6G shall intensify the support of a massive number of low-power and low-complexity devices, but with some spectral efficiency demands [1], [2]. Such use case is especially important for the Internet of Things (IoT), where the complexity of network infrastructure, spectrum allocation, and service management increase drastically. Even more challenging are multi-operator IoT networks, so that authentication, authorization, and accounting become highly complex and nearly intractable [3].

Distributed ledger technologies, as blockchain, bring high hopes to provide scalable decentralized applications and offloading computing, while dealing with limited resources in terms of computing capability, storage, memory, and energy [4], [5]. This technology is envisioned as one of the key enablers of 6G [1]–[3], specially for IoT applications and multi-operator trustless scenarios. In [3], [6], [7], the blockchain radio access network (B-RAN) paradigm is

proposed as a means to build a large cooperative network formed by several smaller networks from different operators, in a trustless environment, yielding multiple benefits. An advantage of B-RAN is the absence of a decentralized control mechanism, relying on the inherent trust and privacy characteristics of blockchain. Moreover, B-RAN also enables independent operators to provide authentication and authorization, facilitating roaming across networks and operators.

Among the several innovative technologies that are spread among the layers comprising the B-RAN paradigm are: trust-free service, inter-host coordination, intelligent consensus, two-tier chain, and trustworthy access [7]. The first four technologies make explicitly use of smart contracts and blockchain. Very recently, in [8] the authors presented a mathematical analysis of the latency induced by updating and reading the blockchain that stores and control service authorizations, while assuming that access requests arrive at a given rate, therefore, focusing only on the upper layers, while abstracting the channel access performance. However, if the channel access method does not perform well, accepting a reduced number of access requests per unit of time, then even if the blockchain at the upper layers can reach consensus in an acceptable time the system performance would be limited.

Blockchain builds trust among multiple service providers and clients in the upper layers of the B-RAN, but does not guarantee that in the lower layers. Trustworthy channel access in the B-RAN is obtained by means of the hash access (HA) protocol [6], [7], in order to manage the access of multi-operator devices to a common access point (AP). In a trustless multi-operator scenario, the selfish behavior of the devices may jeopardize the network performance [6]. In an attempt to solve this issue, in the HA protocol the AP periodically broadcasts access contracts with a set of parameters, the service fee and a target hash. Then, before data transmission, each device must compute a valid hash value by combining the parameters advertised by the AP, being enabled to transmit in that time slot only if the calculated hash value is below the target. Furthermore, a service-before-payment mechanism is usually employed through the blockchain framework, so that the service fee specified in the smart contract is automatically transferred from the device to the operator of that AP, providing short-delay network access [3]. However, since the hash value is individually calculated in a decentralized fashion by the devices, more than one device can potentially obtain a valid hash value in the same time slot, accessing the channel concurrently and creating collisions not handled by the HA protocol, resulting in the loss of the collided messages and harming the throughput.

Manuscript received January 11, 2021; accepted February 2, 2021. Date of publication February 4, 2021; date of current version May 10, 2021. This work was supported in part by CAPES, Brazil, Finance Code 001, PrInt CAPES-UFSC “Automation 4.0” and in part by CNPq, Brazil. The associate editor coordinating the review of this article and approving it for publication was Y. Zhu. (Corresponding author: Glauber Brante.)

Jamil Farhat, Jorge Felipe Grybosi, and Glauber Brante are with the CPGEI, Federal University of Technology-Paraná, Curitiba 80230-901, Brazil (e-mail: jfarhat@alunos.utfpr.edu.br; jgrybosi@alunos.utfpr.edu.br; gbrante@utfpr.edu.br).

Richard Demo Souza is with the Department of Electrical Engineering, Federal University of Santa Catarina, 88034500 Florianópolis, Brazil (e-mail: richard.demo@ufsc.br).

João Luiz Rebelatto is with the DAELN, Federal University of Technology-Paraná, 80230-901 Curitiba, Brazil (e-mail: jlrebelatto@utfpr.edu.br).

Digital Object Identifier 10.1109/LWC.2021.3057264

TABLE I
LIST OF SYMBOLS ADOPTED IN THIS LETTER

Symbol	Definition	Symbol	Definition	Symbol	Definition	Symbol	Definition
α	Path-loss exponent	r	Distance device-AP	P	Transmission power	h	Fading coefficient
N	Overall number of devices	N_{HA}	Number of enabled devices	R	Radius of the area	k_{target}	Target hash value
k_{max}	Maximum k_{target}	κ	Difficulty	κ_*	Optimal difficulty	ρ	Throughput
$\bar{\rho}$	Average SNR	ϱ	Instantaneous SNR	P_{out}	Outage probability	ξ	Target rate

TABLE II
LIST OF ACRONYMS ADOPTED IN THIS LETTER

Acronym	Meaning
AP	Access Point
B-RAN	Blockchain Radio Access Network
CDF	Cumulative Density Function
HA	Hash Access
IoT	Internet-of-Things
SNR	Signal-to-Noise Ratio
NOHA	Non-Orthogonal Hash Access
NOMA	Non-Orthogonal Multiple Access
PDF	Probability Density Function
SIC	Successive Interference Cancellation

In this letter, we extend the HA protocol to allow concurrent transmissions when two devices with a valid hash value transmit in the same time slot. To that end, we employ non-orthogonal multiple access (NOMA) in the power domain along with successive interference cancellation (SIC) [9] at the AP. The contributions of this letter are: i) we obtain the analytical expressions of the outage probability and the throughput of the HA protocol; ii) we introduce the non-orthogonal hash access (NOHA) scheme, which resorts to SIC aiming to resolve collisions of packets that would be discarded by the HA protocol. The outage probability and the throughput of the proposed NOHA scheme are analytically obtained; iii) we provide a closed form to the optimal difficulty to access the channel that maximizes the network throughput.

Notation: Throughout this letter, $f_x(\cdot)$ and $F_x(\cdot)$ refer respectively to the probability density function (PDF) and cumulative density function (CDF) of a given random variable x . Moreover, $\gamma(a, b)$ is the lower incomplete gamma function while $\Pr\{\Phi\}$ corresponds to the probability of event Φ . The main symbols and acronyms adopted in this letter are summarized in Table I and Table II, respectively.

II. SYSTEM MODEL

We consider the uplink of a wireless network where N devices, uniformly distributed in a circular area of radius R , have independent information to transmit to a common AP in the center of the area. The devices are delay tolerant, transmitting with a low probability, and share the wireless channel through the grant-free HA protocol. This is illustrated in Fig. 1. The number of devices concurrently enabled to transmit is $N_{\text{HA}} \ll N$ [6]. In the example provided in Fig. 1, for instance, one has that $N_{\text{HA}} = 1$. Moreover, we adopt a time-slotted model where synchronism is established through beacons periodically broadcasted by the AP.¹ Due to the potential simultaneous transmission of more than one device, the

¹Note that this is a common requirement of time-slotted models, not demanding additional overhead when compared to slotted Aloha, for example.

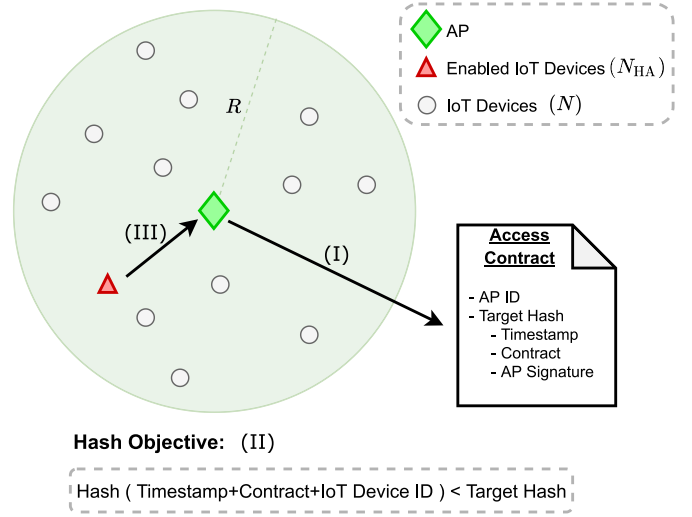


Fig. 1. System model and block diagram of Hash Access (HA) protocol [6].

signal received at the AP in a given time slot (whose index is omitted for convenience) can be written as

$$\mathbf{y} = \sum_{i=1}^{N_{\text{HA}}} \sqrt{r_i^{-\alpha} P} h_i \mathbf{x}_i + \mathbf{w}, \quad (1)$$

where r_i is the distance between the AP and the i -th transmitting IoT node, α is the path-loss exponent, P is the transmit power, assumed to be the same for all devices, \mathbf{x}_i is the signal vector transmitted over a complex-Gaussian channel with zero mean and unity-variance whose envelop $|h_i|$ follows a Rayleigh distribution, and \mathbf{w} is the zero-mean complex Gaussian noise vector with variance σ^2 .

III. HASH ACCESS (HA) PROTOCOL

The HA is a trustworthy grant-free access scheme where, before accessing the channel and starting transmitting, the device willing to transmit shall successfully solve a hash puzzle [6]. The main steps of the HA protocol are illustrated in Fig. 1 and described as: (I) the access contract is broadcast by the AP; (II) the hash value is calculated by devices willing to access the channel, which, besides the contract itself, depends on a timestamp and the device ID; (III) the devices that obtained a valid hash value access the channel.

A. Difficulty to Access the Channel

Let $k_{\text{target}} \in \mathbb{Z}$ represent the target hash value, which belongs to the interval from 0 to a given maximum value $k_{\text{max}} \in \mathbb{Z}$. Assuming that the hash values obtained in different attempts made by the i th IoT device are uniformly

distributed, we have that $\Pr\{k_i < k_{\text{target}}\} = \frac{k_{\text{target}}}{k_{\text{max}}+1} \forall i$, where k_i represents the hash value computed by device i .

Definition 1 (Difficulty): The difficulty κ is defined as the probability of obtaining an invalid hash value, i.e.,:

$$\kappa = \Pr\{k_i \geq k_{\text{target}}\} = 1 - k_{\text{target}}/(k_{\text{max}} + 1). \quad (2)$$

The larger the difficulty in (2), the harder is to access the channel. Note that, if κ is oversized by the AP, there might exist vacant time slots, which are wasted without any hash-enabled device to transmit. On the other hand, small values of κ may lead to an excessive number of collisions, whose collided packets are discarded [6]. It becomes then of paramount importance to adjust the value of κ such that, with high probability, only a single device computes a valid hash value per time slot.

Let us define N_{HA} as the number of devices that found a hash value below the target in a given time slot. The probability of N_{HA} being equal to $n \in [0, N]$ is then

$$\Pr\{N_{\text{HA}} = n\} = \binom{N}{n} (1 - \kappa)^n \kappa^{N-n}. \quad (3)$$

Since HA requires that $N_{\text{HA}} = 1$ (if $N_{\text{HA}} = 0$ there is no transmission and if $N_{\text{HA}} > 1$ the packets are lost due to collision), it can be shown that the optimal value of κ that maximizes $\Pr\{N_{\text{HA}} = 1\}$ in (3) is given by

$$\kappa_{\star}^{(\text{HA})} = (N - 1)/N. \quad (4)$$

B. Outage Probability of HA

In this interference-free scenario with $N_{\text{HA}} = 1$, the average signal-to-noise ratio (SNR) is obtained with the aid of (1) as

$$\bar{\varrho}_i = (r_i^{-\alpha} P)/\sigma^2, \quad (5)$$

being the instantaneous SNR given by $\varrho_i = |h_i|^2 \bar{\varrho}_i$. The point-to-point outage probability between device i and the AP is defined as the probability that the instantaneous SNR falls below a threshold that allows correct decoding, i.e., $\Pr\{\varrho_i < \varrho_0\}$, where $\varrho_0 = 2^\xi - 1$ if we consider the Shannon capacity [10], with ξ being the target rate (in bps/Hz).

Therefore, the average outage probability depends on the spatial distribution of the devices. The probability density function (PDF) of the distance between a uniformly distributed device and the centralized AP is $f_R(r) = 2r/R^2$ [11, Proposition 2]. The probability of ϱ_i being no lower than the threshold ϱ_0 is obtained from the cumulative distribution function (CDF)

$$F_\varrho(\varrho_0, \alpha, r) = \Pr\{\varrho_i \geq \varrho_0\} = \exp\left(-\frac{\varrho_0 \sigma^2}{r^{-\alpha} P}\right). \quad (6)$$

Then, averaging (6) with respect to r , we have

$$\begin{aligned} F_\varrho(\varrho_0, \alpha) &= 1 - \int_0^R f_R(r) F_\varrho(\varrho_0, \alpha, r) \, dr \\ &= 1 - \frac{2}{R^2} \int_0^R r \exp\left(-\frac{\varrho_0 \sigma^2}{r^{-\alpha} P}\right) \, dr \\ &\stackrel{(a)}{=} \frac{\gamma(2/\alpha, \varrho_0 \sigma_P^2 R^\alpha)}{\alpha (\varrho_0 \sigma_P^2)^{2/\alpha}}, \end{aligned} \quad (7)$$

where $\sigma_P^2 = \sigma^2/P$, $\gamma(\cdot, \cdot)$ is the lower incomplete gamma function and (a) is obtained with the aid of [12, eq. (3.381.8)].

A successful transmission between a device and the AP in the HA protocol has two requirements: i) there might be no collision at all (event whose probability is $\Pr\{N_{\text{HA}} = 1\}$ from (3)); and ii) the communication link needs to be in favorable conditions, not in outage (which happens with probability $F_\varrho(\varrho_0, \alpha)$ from (7)). The average outage probability of the HA protocol is then complementarily obtained as:

$$\begin{aligned} P_{\text{out}}^{(\text{HA})} &= 1 - \Pr\{N_{\text{HA}} = 1\} F_\varrho(\varrho_0, \alpha) \\ &= 1 - N(1 - \kappa) \kappa^{N-1} \left[\frac{\gamma(2/\alpha, \varrho_0 \sigma_P^2 R^\alpha)}{\alpha (\varrho_0 \sigma_P^2)^{2/\alpha}} \right]. \end{aligned} \quad (8)$$

C. Throughput of HA

The throughput is the average outage-free transmission rate,

$$\rho^{(\text{HA})} = \xi \left(1 - P_{\text{out}}^{(\text{HA})}\right) \quad [\text{bps/Hz}]. \quad (9)$$

It can be shown that the throughput from (9) is maximized by adopting the optimal difficulty $\kappa_{\star}^{(\text{HA})}$ from (4). However, although $\kappa_{\star}^{(\text{HA})}$ maximizes $\rho^{(\text{HA})}$ by maximizing $\Pr\{N_{\text{HA}} = 1\}$ (i.e., reducing the number of collisions as much as possible), there is still a non negligible probability that $N_{\text{HA}} > 1$. More specifically, $\Pr\{N_{\text{HA}} = 1\} \rightarrow 1/e \approx 0.368$ when adopting $\kappa_{\star}^{(\text{HA})}$ with $N \rightarrow \infty$, which coincides with the maximum throughput achieved by the slotted ALOHA protocol [10]. Thus, one has that in average approximately 63.2% of the time slots are discarded due to collisions, compromising the throughput.

IV. NON-ORTHOGONAL HASH ACCESS (NOHA)

In the proposed NOHA scheme, we consider that the AP is capable of dealing at most with $N_{\text{HA}} = 2$ concurrent transmissions at the same time slot. If $N_{\text{HA}} > 2$, then we assume that all the colliding packets are discarded by the AP.²

If the number of transmitting devices is $N_{\text{HA}} = 1$, then NOHA behaves as the HA scheme, since there is no collision. However, when $N_{\text{HA}} = 2$, the AP tries to recover the packets transmitted by both devices employing SIC [9]. To that end, let us say that the instantaneous SNR of the two colliding packets are given by ϱ_1 and ϱ_2 , which are realizations of independent and identically distributed (i.i.d.) random variables. Upon receiving a collided packet, the AP first tries to decode the user with the highest instantaneous SNR, while treating the other user as interference. In case of successful decoding, the signal of such user is removed from the superimposed signal, and the AP then tries to decode the other device. The process is interrupted either after correctly decoding both devices or upon finding the first device in outage.

A. Outage Probability of SIC

Without loss of generality, we define $\varrho_s = \max\{\varrho_1, \varrho_2\}$ and $\varrho_w = \min\{\varrho_1, \varrho_2\}$ as the instantaneous SNR of the stronger and the weaker devices, respectively. In the first iteration of

²This is in accordance to the typical low complexity of IoT networks, since performing multiple SIC iterations may be very complex.

the SIC process, the signal to interference plus noise ratio (SINR) experienced at the AP is $\varrho_s/(1+\varrho_w)$, since the weaker device is treated as interference. Thus, the stronger user is correctly recovered with probability $\Pr\{\varrho_s \geq \varrho_0(1+\varrho_w)\}$. The weaker user, in turn, is correctly recovered with probability $\Pr\{\varrho_s \geq \varrho_0(1+\varrho_w) \cap \varrho_w \geq \varrho_0\}$, since the second iteration is free of interference and depends on the success of the first iteration.

The outage probability of the first SIC iteration is [9]

$$P_{\text{out,iter 1}}^{(\text{NOHA})} = \Pr\{\varrho_s < \varrho_0(1+\varrho_w)\} \\ = \int_0^\infty \int_{\varrho_w}^{\varrho_0(1+\varrho_w)} f_{\varrho}(\varrho_w) f_{\varrho}(\varrho_s) d\varrho_s d\varrho_w. \quad (10)$$

However, (10) is mathematically intractable in the present form. Thus, we first consider the particular and practical case of $\alpha = 4$ in (7), which reduces the CDF to

$$F_{\varrho}(\varrho_0, 4) = \frac{\sqrt{\pi} \operatorname{erf}\left(R^2 \sqrt{\varrho_0 \sigma_P^2}\right)}{2 R^2 \sqrt{\varrho_0 \sigma_P^2}}. \quad (11)$$

Then, we approximate (11) by applying a Gaussian-Chebyshev quadrature following [13], as

$$F_{\varrho}(\varrho_0, 4) \approx \frac{\pi}{2L} \sum_{l=1}^L \beta_l \left[1 - \exp\left(-c_l \varrho_0 \sigma_P^2\right)\right], \quad (12)$$

where L defines the approximation complexity-accuracy trade-off [13], while $\beta_l = \sqrt{(1-\theta_l^2)}(\theta_l+1)$, $c_l = 1 + (\frac{R}{2}\theta_l + \frac{R}{2})^\alpha$ and $\theta_l = \cos(\frac{2l-1}{2L}\pi)$. The PDF associated with (12) is then

$$f_{\varrho}(\varrho_0) \approx \frac{\pi}{2L} \sum_{l=1}^L \beta_l c_l \exp\left(-c_l \varrho_0 \sigma_P^2\right). \quad (13)$$

After combining (10) and (13) one can show that the outage probability of the first iteration of the SIC process becomes

$$P_{\text{out,iter 1}}^{(\text{NOHA})} \approx \sum_{n=1}^L \sum_{k=1}^L \left[\frac{1}{c_n + c_k} - \frac{\exp(-c_k \varrho_0 \sigma_P^2)}{c_n + c_k \varrho_0} \right] \\ \times \frac{\pi^2 c_n (1+\theta_n)(1+\theta_k)}{2 L^2 (1-\theta_n^2)^{-\frac{1}{2}} (1-\theta_k^2)^{-\frac{1}{2}}}. \quad (14)$$

The outage probability of the second iteration given that the first iteration is successful can be obtained as

$$P_{\text{out,iter 2|1}}^{(\text{NOHA})} = \Pr\{\varrho_w = \min\{\varrho_1, \varrho_2\} < \varrho_0\} \\ \stackrel{(a)}{=} 2 F_{\varrho}(\varrho_0, \alpha) + [F_{\varrho}(\varrho_0, \alpha)]^2. \quad (15)$$

where (a) holds due to the property of the minimum between two i.i.d. random variables [14]. Finally, the average outage probability after the second iteration of the SIC decoder is

$$P_{\text{out,iter 2}}^{(\text{NOHA})} = 1 - \Pr\{\varrho_s \geq \varrho_0(1+\varrho_w) \cap \varrho_w \geq \varrho_0\} \\ \stackrel{(a)}{\approx} 1 - \left(1 - P_{\text{out,iter 1}}^{(\text{NOHA})}\right) \left(1 - P_{\text{out,iter 2|1}}^{(\text{NOHA})}\right), \quad (16)$$

where (a) assumes mutual independent events as in [9].

B. Throughput of the NOHA Scheme

The throughput of NOHA depends on N_{HA} , being

$$\rho^{(\text{NOHA})} = \xi \Pr\{N_{\text{HA}} = 1\} F_{\varrho}(\varrho_0, \alpha) \\ + \xi \Pr\{N_{\text{HA}} = 2\} \left(1 - P_{\text{out,iter 1}}^{(\text{NOHA})}\right) P_{\text{out,iter 2|1}}^{(\text{NOHA})} \\ + 2\xi \Pr\{N_{\text{HA}} = 2\} \left(1 - P_{\text{out,iter 2}}^{(\text{NOHA})}\right), \quad (17)$$

where the first term represents the situation where only a single device accesses the channel, being equal to $\rho^{(\text{HA})}$ from (9); the second term stands for the NOMA of two users, but only the first iteration of the SIC process is successful, while the third term represents the situation where both colliding users have been correctly recovered by SIC.

1) *Optimal κ That Maximizes the Throughput:* From (17) and (3), we observe that only the access probabilities $\Pr\{N_{\text{HA}} = n\}$ depend on κ , while the outage probabilities depend only on the channel and transmit power. Therefore, since $\rho^{(\text{NOHA})}$ is a linear combination of $\Pr\{N_{\text{HA}} = n\}$ for $n = \{1, 2\}$, one can conclude that (17) is convex by realizing that (3) is convex [15]. The goal is then to find

$$\kappa_{\star}^{(\text{NOHA})} = \underset{\kappa}{\operatorname{argmax}} \rho^{(\text{NOHA})}. \quad (18)$$

Since the throughput in (17) is convex with respect to κ , one can obtain $\kappa_{\star}^{(\text{NOHA})}$ by solving $\partial \rho^{(\text{NOHA})} / \partial \kappa = 0$, yielding

$$\kappa_{\star}^{(\text{NOHA})} = \frac{1}{2N(\phi_1 - \phi_2)} \left[(N-1)(\phi_1 - 2\phi_2) \right. \\ \left. + \sqrt{4\phi_2(\phi_2 - \phi_1) + \phi_1^2(N-1)^2} \right], \quad (19)$$

where $\phi_2 = \xi \binom{N}{2} (1 - P_{\text{out,iter 1}}^{(\text{NOHA})})(2 - P_{\text{out,iter 2|1}}^{(\text{NOHA})})$ and $\phi_1 = \xi N F_{\varrho}(\varrho_0, \alpha)$.

Note that the optimal difficulty from (19) depends basically on the number of devices, target rate and outage performance of the SIC process.

V. NUMERICAL RESULTS

We provide numerical examples comparing the proposed NOHA protocol with HA [6]. Unless stated otherwise, we assume $\alpha = 4$, $R = 100$ m and $\sigma^2 = -104$ dBm [11]. Other parameters such as P , κ and N have been arbitrarily chosen for every particular scenario, aiming at covering a wide range of values. Fig. 2 compares the analytical throughput from (17) when adopting the approximations from (14) and (16) to exact simulation results. It can be seen that, despite a slight deviation as P and ξ increase, the analysis accurately matches the numerical results. Moreover, it is important to remark that in a typical scenario of massive IoT ξ is small, closer to 1 than to 5 bps/Hz.

The influence of the difficulty in the throughput is evaluated in Fig. 3. One can see that, for a fixed value of ξ , NOHA outperforms the HA scheme across the entire range of κ . Another interesting remark is that $\kappa_{\star}^{(\text{NOHA})} < \kappa_{\star}^{(\text{HA})}$, i.e., NOHA presents a lower optimal difficulty than HA, allowing on average a higher number of devices to transmit concurrently. This is due to the SIC capability of recovering collisions. Finally, it can be seen that, despite the small throughput deviation for $\xi > 1$ as illustrated in Fig. 2, the optimal difficulty

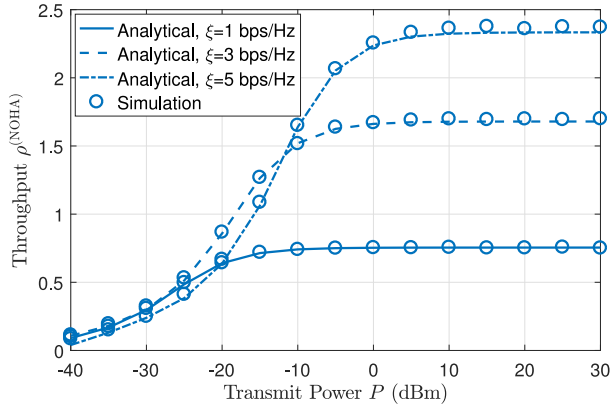


Fig. 2. Throughput of the NOHA protocol as a function of P with $N = 20$ IoT devices, $\kappa = 0.95$ and $\xi \in \{1, 3, 5\}$ bps/Hz.

TABLE III
RELATIVE GAIN $\rho^{(\text{NOHA})}/\rho^{(\text{HA})}$ FOR κ_* , $N = 20$ AND $P = 0$ dBm

ξ (bps/Hz)	0.5	1	3	5
$\rho^{(\text{NOHA})}/\rho^{(\text{HA})}$	2.31	2.30	1.60	1.27

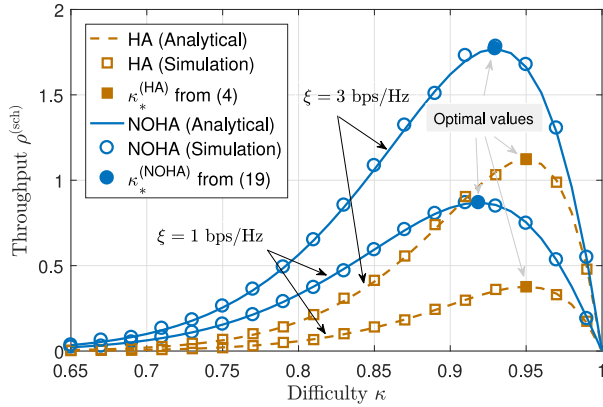


Fig. 3. Throughput of HA and NOHA vs. κ , for $N = 20$ and $P = 0$ dBm.

$\kappa_*^{(\text{NOHA})}$ obtained from (19) is accurately supported by the simulations even in the scenario with larger rates (in this example $\xi = 3$ bps/Hz).

Table III lists the relative gain of NOHA over HA, $\rho^{(\text{NOHA})}/\rho^{(\text{HA})}$, when adopting κ_* for each method, and with $N = 20$, for different values of ξ . The gain is larger for low ξ , typical of massive IoT scenarios, being as much as 2.31 for $\xi = 0.5$ bps/Hz, but diminishes with ξ due to the difficulty of performing a successful SIC when a collision happens.

Fig. 4 illustrates the influence of N , either with fixed $\kappa = 0.9$ or the optimal $\kappa_*^{(\text{HA})}$ from (4) and $\kappa_*^{(\text{NOHA})}$ from (19). By adapting the difficulty as the number of devices varies, the throughput remains almost constant, so that the floor achieved by NOHA is more than double of that achieved by HA.

VI. CONCLUSION

We elaborated on the recently introduced HA-based protocol for blockchain radio access networks (B-RANs). In the new non-orthogonal hash access (NOHA) scheme, the AP employs successive interference cancellation (SIC) in a non-orthogonal multiple access protocol, dealing with collisions

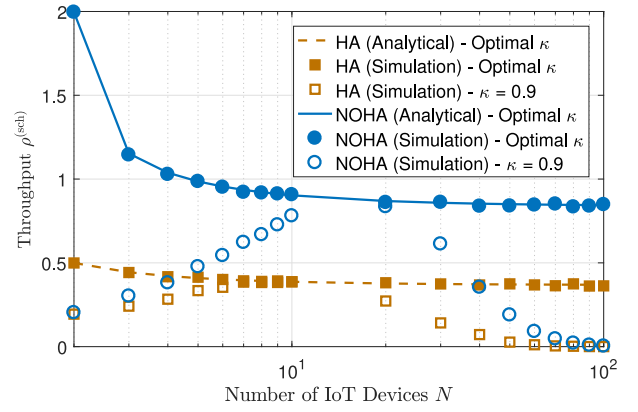


Fig. 4. Throughput of the HA and NOHA protocols as a function of N , for $P = 0$ dBm, $\xi = 1$ bps/Hz and when adopting the optimal difficulty.

not handled by the standard HA protocol. The difficulty in accessing the channel that maximizes the network throughput is obtained analytically, matching the numerical results and showing that the proposed NOHA scheme can increase the network throughput in more than 100% when compared to HA.

REFERENCES

- [1] "Key drivers and research challenges for 6G ubiquitous wireless intelligence, 6G research visions 1," 6G Flagship, Univ. Oulu, Oulu, Finland, Rep. 1, Sep. 2019.
- [2] F. Tariq, M. R. A. Khandaker, K.-K. Wong, M. A. Imran, M. Bennis, and M. Debbah, "A speculative study on 6G," *IEEE Wireless Commun.*, vol. 27, no. 4, pp. 118–125, Aug. 2020.
- [3] X. Ling, J. Wang, T. Bouchoucha, B. C. Levy, and Z. Ding, "Blockchain radio access network (B-RAN): Towards decentralized secure radio access paradigm," *IEEE Access*, vol. 7, pp. 9714–9723, 2019.
- [4] T. Maksymyuk *et al.*, "Blockchain-empowered framework for decentralized network management in 6G," *IEEE Commun. Mag.*, vol. 58, no. 9, pp. 86–92, Sep. 2020.
- [5] Z. Li, M. Xu, J. Nie, J. Kang, W. Chen, and S. Xie, "NOMA-enabled cooperative computation offloading for blockchain-empowered Internet of Things: A learning approach," *IEEE Internet Things J.*, early access, Aug. 14, 2020, doi: [10.1109/JIOT.2020.3016644](https://doi.org/10.1109/JIOT.2020.3016644).
- [6] X. Ling, Y. Le, J. Wang, and Z. Ding, "Hash access: Trustworthy grant-free IoT access enabled by blockchain radio access networks," *IEEE Netw.*, vol. 34, no. 1, pp. 54–61, Jan./Feb. 2020.
- [7] X. Ling, J. Wang, Y. Le, Z. Ding, and X. Gao, "Blockchain radio access network beyond 5G," *IEEE Wireless Commun.*, vol. 27, no. 6, pp. 160–168, Dec. 2020.
- [8] X. Ling, Y. Le, J. Wang, Z. Ding, and X. Gao, "Practical modeling and analysis of blockchain radio access network," *IEEE Trans. Commun.*, early access, Oct. 9, 2020, doi: [10.1109/TCOMM.2020.3029779](https://doi.org/10.1109/TCOMM.2020.3029779).
- [9] Y. Gao, B. Xia, K. Xiao, Z. Chen, X. Li, and S. Zhang, "Theoretical analysis of the dynamic decode ordering SIC receiver for uplink NOMA systems," *IEEE Commun. Lett.*, vol. 21, no. 10, pp. 2246–2249, Oct. 2017.
- [10] A. Goldsmith, *Wireless Communications*, 1st ed. Cambridge, U.K.: Cambridge Univ. Press, 2005.
- [11] Y. Sun, L. Zhang, G. Feng, B. Yang, B. Cao, and M. A. Imran, "Blockchain-enabled wireless Internet of Things: Performance analysis and optimal communication node deployment," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 5791–5802, Jun. 2019.
- [12] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, 7th ed. Amsterdam, The Netherlands: Elsevier/Academic, 2007.
- [13] M. Abramowitz and I. Stegun, *Handbook of Mathematical Functions, With Formulas, Graphs, and Mathematical Tables*. New York, NY, USA: Dover Publ., Inc., 1974.
- [14] A. Papoulis and S. Pillai, *Probability, Random Variables, and Stochastic Processes*, 4th ed. Boston, MA, USA: McGraw-Hill Higher Educ., 2002.
- [15] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, U.K.: Cambridge Univ. Press, 2004.