Random Access Analysis for Massive IoT Networks under A New Spatio-Temporal Model: A Stochastic Geometry Approach

Nan Jiang, Yansha Deng, Xin Kang, and Arumugam Nallanathan

Abstract

Massive Internet of Things (mIoT) has provided an auspicious opportunity to build powerful and ubiquitous connections that faces a plethora of new challenges, where cellular networks are potential solutions due to their high scalability, reliability, and efficiency. The Random Access CHannel (RACH) procedure is the first step of connection establishment between IoT devices and Base Stations (BSs) in the cellular-based mIoT network, where modeling the interactions between static properties of physical layer network and dynamic properties of queue evolving in each IoT device are challenging. To tackle this, we provide a novel traffic-aware spatio-temporal model to analyze RACH in cellular-based mIoT networks, where the physical layer network is modeled and analyzed based on stochastic geometry in the spatial domain, and the queue evolution is analyzed based on probability theory in the time domain. For performance evaluation, we derive the exact expressions for the preamble transmission success probabilities of a randomly chosen IoT device with different RACH schemes in each time slot, which offer insights into effectiveness of each RACH scheme. Our derived analytical results are verified by the realistic simulations capturing the evolution of packets in each IoT device. This mathematical model and analytical framework can be applied to evaluate the performance of other types of RACH schemes in the cellular-based networks by simply integrating its preamble transmission principle.

I. INTRODUCTION

Massive Internet of Things (mIoT) is deemed to connect billions of miscellaneous mobile devices or IoT devices that empowers individuals and industries to achieve their full potential. A plethora of new applications, such as autonomous driving, remote health care, smart-homes, smart-grids, and etc, are being innovated via mIoT, in which ubiquitous connectivities among massive IoT devices are operated fully automatedly without human intervention. The successful

N. Jiang, Y. Deng and A. Nallanathan are with Department of Informatics, King's College London, London, UK (e-mail:{nan.3.jiang, yansha.deng, arumugam.nallanathan}@kcl.ac.uk). (Corresponding author: Yansha Deng (e-mail:yansha.deng@kcl.ac.uk).)

X. Kang is with National Key Laboratory of Science and Technology on communications, University of Electronic Science and Technology of China, Chengdu, 611731, Sichuan, China (e-mail: kangxin83@gmail.com).

operation of these IoT applications faces various challenges, among them providing wireless access for the tremendous number of IoT devices has been considered to be the main problem. This issue has been regarded as one of key differences between mIoT and human-to-human (H2H) wireless communication networks, such that the conventional H2H communication architecture needs to be adjusted to support the mIoT networks.

Previously, cellular network (e.g, Long Term Evolution (LTE)) and short-range transmission technologies (e.g, ZigBee, Bluetooth) were considered as potential solutions to support mIoT networks, however none of them can achieve all wide coverage, low power consumption and supporting massive IoT devices at the same time [1–4]. To solve this, Low-Power Wide Area Networks (LPWANs) is proposed as an alternative solution for mIoT networks that enables the operation in the unlicensed band (e.g, LoRa, Sigfox) and licensed band (e.g, extended coverage GSM-IoT, enhanced machine type communication, and narrow band IoT (NB-IoT)). According to the Third Generation Partnership Project (3GPP), the IoT technologies are suggested to be developed based on the existing cellular infrastructure, due to its low additional hardware deployment cost as well as high-level of security by operating on the licensed band [3–9].

In the cellular-based mIoT network, connections between IoT device with BS are provided by incorporating these IoT devices in existing cellular networks directly or via IoT gateways. In this network, the number of IoT devices is expected to raise up to more than thirty thousands per cell and such IoT devices may request access simultaneously for their small size data packets uplink transmission [5, 10, 11]. As such improving the access mechanisms of current cellular systems is one of key challenges for the cellular-based mIoT network [3–7, 12]. In LTE, a device performs Random Access CHannel (RACH) procedure when it needs to establish or re-establish a data connection with its associated BS, and the first step of RACH is that the device transmits a preamble via physical random access channel (PRACH) [13]. Two ways exist for accessing to the network: 1) the contention-free RACH for delayed-constrained access requests (e.g, handover), where the BS distributes one of the reserved dedicated preamble to a device, and then the device uses its dedicated preamble to initiate a contention-free RACH; 2) the contention-based RACH for delay-tolerant access requests (e.g, data transmission), where an IoT device randomly chooses a preamble from non-dedicated preambles to transmit to its associated BS [13]. Generally, the contention-based RACH is much more sensitive to IoT traffic [3, 4, 12], such that most works have analyzed its scalability characteristics in supporting massive concurrent access requests [14–20].

The contention-based RACH has been widely studied in the conventional LTE networks, where the most critical point of this issue concerns modeling and analyzing time-varying queues and RACH schemes in MAC layer [21, 22]. Recently, a number of studies have been launched to discuss whether the contention-based RACH of LTE is suitable for mIoT, and how to evolve cellular systems to provide efficient access for mIoT networks [4, 17, 19, 20]. In [17], the authors developed a MAC-level model for the four-step RACH procedure to analyze and compare the baseline scheme and the dynamic back-off scheme. In [19], a novel Access Class Barring (ACB) scheme is proposed with a constant association rate. In [20], the authors devolop analytical models for the spatial-randomization ACB scheme and the time-spatial randomization, as well as compare them with the 3GPP specified eNodeB-employed time-randomization ACB scheme. However, in [17, 19–22], the collision events are considered as the main outage condition, and the preamble transmission failure impacted by the physical channel propagation characteristics is simplified. Generally speaking, in the large-scale cellular-based mIoT network, the physical layer characteristics can strongly influence the performance of RACH success, due to that the received signal-to-interference-plus-noise ratio (SINR) at the BS can be severely degraded by the mutual interference generated from massive IoT devices. In this scenario, the random positions of the transmitters make accurate modeling and analysis of this interference even more complicated.

Stochastic geometry has been regarded as a powerful tool to model and analyze mutual interference between transceivers in the wireless networks, such as conventional cellular networks [23–25], wireless sensor networks [26], cognitive radio networks [27, 28], and heterogenous cellular networks [29–31]. However, there are two aspects that limit the application of conventional stochastic geometry analysis to the RACH analysis of the cellular-based mIoT networks: 1) conventional stochastic geometry works focused on analyzing normal uplink and downlink data transmission channel, where the intra-cell interference is not considered, due to the ideal assumption that each orthogonal sub-channel is not reused in a cell, whereas massive IoT devices in a cell may randomly choose and transmit the same preamble using the same sub-channel; 2) these conventional stochastic geometry works only modeled the spatial distribution of transceivers, and ignored the interactions between static properties of physical layer network and the dynamic properties of queue evolving in each transmitter due to the assumptions of backlogged network with saturated queues [32–34].

To model these aforementioned interactions, recent works have studied the stability of spatially spread interacting queues in the network based on stochastic geometry and queuing theory [31–

34]. The work in [32] is the first paper applying the stochastic geometry and queuing theory to analyze the performance of RACH in distributed networks, where each transmitter is composed of an infinite buffer, and its location is changed following a high mobility random walk. The work in [33] investigated the stable packet arrival rate region of a discrete-time slotted RACH network, where the transceivers are static and distributed as independent Poisson point processes (PPPs). The work in [31] analyzed the delay in the heterogeneous cellular networks with spatio-temporal random arrival of traffic, where the traffic of each device is modeled by a marked Poisson process, and the statistics of such traffic with different offloading policies are compared. In [34], the authors have modeled the randomness in the locations of IoT devices and BSs via PPPs, and leveraged the discrete time Markov chain to model the queue and protocol states of each IoT device. However, the model is limited in capturing the dynamic preamble success probability during the time evolution, such that it can only derive the analytical result during the steady state, and this result is unable to be verified by simulations.

In this paper, we develop a novel spatio-temporal mathematical framework for cellular-based mIoT network using stochastic geometry and probability theory, where the BSs and IoT devices are modeled as independent PPPs in the spatial domain. In the time domain, the new arrival packets of each IoT device are modeled by independent Poisson arrival processes [15, 31, 35, 36]. The packets status in each IoT device that are jointly populated by the new Poisson arrival packets and the accumulated packets in the previous time slots according to its stochastic geometry analysis, determines the aggregate interference at the received SINR in the current time slot, which then determines the non-empty probability and non-restrict probability of IoT device (i.e., IoT device have back-logged packets and permission to transmit currently) in the current time slot. The contributions of this paper can be summarized in the following points:

- We present a novel spatio-temporal mathematical framework for analyzing contention-based RACH of the mIoT network. Assuming the independent Poisson arrival, the packets accumulation and preamble transmission of a typical IoT device in each time slot is accurately modeled.

- With single time slot, we derive the exact expressions for the preamble detection probability of a randomly chosen BS, the preamble transmission success probability of a randomly chosen IoT device, and the number of received packets per BS in the cellular-based mIoT networks.

- With multiple time slots, the queue statuses are firstly analyzed based on probability theory,

and then approximated by their corresponding Poisson arrival distributions, which facilitates the queuing analysis. By doing so, we derive the exact expressions for the preamble transmission success probability of a randomly chosen IoT device in each time slot with the baseline, the ACB, and the back-off schemes for their performance comparison.

- We develop a realistic simulation framework to capture the randomness location, preamble tranmission, and the real packets arrival, accumulation, and departure of each IoT device in each time slot, where the queue evolution as well as the stochastic geometry analysis are all verified by our proposed realistic simulation framework.

- The analytical model presented in this paper can also be applied for the performance evaluation of other types of RACH schemes in the cellular-based networks by substituting its preamble transmission principle.

The rest of the paper is organized as follows. Section II presents the network model. Sections III derives preamble detection probability of a randomly chosen BS and the preamble transmission success probability of a randomly chosen IoT device in single time slot. Section IV derives the preamble transmission success probabilities of a randomly chosen IoT device in each time slot with different schemes. Finally, Section V concludes the paper.

II. SYSTEM MODEL

We consider an uplink model for cellular-based mIoT network consists of a single class of base stations (BSs) and IoT devices, which are spatially distributed in $\mathbb{R}^2$ following two independent homogeneous Poisson point process (PPP), Φ_B and Φ_D, with intensities λ_B and λ_D, respectively. Same as [23, 30, 37], we assume each IoT device associates to its geographically closest BS, and thus forms a Voronoi tesselation, where the BSs are uniformly distributed in the Voronoi cell. Same as [31, 33], the time is slotted into discrete time slots, and the number and locations of BSs and IoT devices are fixed all time once they are deployed.

A. Network Description

We consider a standard power-law path-loss model, where the signal power decays at a rate $r^{-\alpha}$ with the propagation distance r, and the path-loss exponent α. We consider Rayleigh fading channel, where the channel power gains $h(x,y)$ between two generic locations $x, y \in \mathbb{R}^2$ is assumed to be exponentially distributed random variables with unit mean. All the channel gains are independent of each other, independent of the spatial locations, and identically distributed (i.i.d.). For the brevity of exposition, the spatial indices (x, y) are dropped.

Uplink power control has been an essential technique in cellular network [23, 30, 38]. We assume that a full path-loss inversion power control is applied at all IoT devices, where each IoT device compensates for its own path-loss to keep the average received signal power equal to a same threshold ρ [34, 39]. By doing so, as a user moves closer to the desired base station, the transmit power required to maintain the same received signal power decreases, which saves energy for battery-powered IoT devices. More importantly, it helps to solve the "near-far" problem, where a BS cannot decode the signals from cell-edge due to high aggregate interference from other nearby IoT devices. The transmit power of ith IoT device P_i depends on the distance from its associated BS, and the defined threshold ρ, where $P_i = \rho r_i^\alpha$. In order to successfully transmit a signal from the IoT device, the maximum transmit power should be high enough for its path-loss inversion, otherwise, it does not transmit the signal and goes into a truncation outage. Here, we assume that the density of BSs is high enough and none of the IoT device suffers from truncation outage (i.e., the transmit power of IoT device is large enough for uplink path-loss inversion, while not violating its own maximum transmit power constraint).

B. Contention-Based Random Access Procedure

In the cellular-based network, the first step to establish an air interface connection is delivering requests to the associated BS via RACH [13], where the contention-based RACH is favored by mIoT network for the initial association to the network, the transmission resources request, and the connection re-establishment during failure [3, 4, 6, 12]. The contention-based RACH has four steps: In step 1, each device randomly chooses a preamble (i.e., orthogonal pseudo code, such as Zadoff-Chu sequence[1]) from avalaible preamble pool, and send to its associated BS via PRACH. In step 2, the IoT device sets a random access response (RAR) window and waits for the BS to response with an uplink grant in the RAR. In step 3, the IoT device that successfully receives its RAR transmits a radio resource control connection request with identity information to BS. In step 4, the BS transmits a RRC Connection Setup message to the IoT device. Note that,

---

[1]In LTE, there are 64 available preambles for RACH in each BS, which are generated on the side of IoT devices from 10 different root sequences [13]. Generally, the preambles generated from the same root are completely orthogonal, and preambles generated from two different roots are nearly orthogonal [13]. To mitigate the interference among preambles generated from different root sequences, some published literature have specifically studied such correlations, and some results shown that their proposed preamble detectors can asymptotically achieve almost interference-free detection performance (i.e., nearly orthogonal) [40]. However, this is beyond the scope of this paper, and to focus on studying spatio-temporal model for RACH, we assume different preambles are completely orthogonal.

only within the step 1 preamble is transmitted via PRACH, but within other steps signals are transmitted via normal uplink and downlink data transmission channel. Further details on the RACH can be found in [13].

In the step 1 of contention-based RACH, the IoT device randomly selects a preamble from a group of non-dedicated preambles defined by the BS. Without loss of generality, we assume that each BS has an available preamble pool with the same number of non-dedicated preambles ξ, known by its associated IoT devices. Each preamble has an equal probability $(1/\xi)$ to be chosen by an IoT device, and the average density of the IoT devices using the same preamble is $\lambda_{Dp} = \lambda_D/\xi$, where the λ_{Dp} is measured with unit devices/preamble/km^2.

In the cellular-based mIoT network, λ_{Dp} is able to be a huge number, due to that the slotted-ALOHA system allows all IoT devices requesting for access in the first available opportunity. Once a huge number of IoT devices transmit preambles simultaneously, the network performance might degrade due to that the preambles cannot be detected or decoded by the BS [3, 4]. Therefore, the contention of preamble in the step 1 becomes one of the main challenges in RACH [5, 16, 17, 34, 41, 42]. Same as [17, 34, 41, 42], we assume that the step 2, 3, and 4 of RA are always successful whenever the step 1 is successful. In other words, the RACH may fail due to the following two reasons: 1) a preamble cannot be recognized by the received BS, due to its low received SINR; 2) the BS successfully received two or more same preambles simultaneously, such that the collision occurs, and the BS cannot decode any collided preambles. In this work, we limit ourselves to single preamble transmission fail same as [33, 34], and leave the collision for our future work, thus we assume that a RACH procedure is always successful if the IoT device successfully transmits the preamble to its associated BS.

C. Physical Random Access CHannel and Traffic Model

We consider a time-slotted mIoT network, where the PRACH happens at the beginning of a time slot within a small time interval τ_c, and the least time of a time slot (i.e., the time between any two PRACHs) is a gap interval duration τ_g for data transmission as shown in Fig. 1. Generally, the PRACH is reserved in the uplink channel and repeated in the system with a certain period that specified by the BS. For instance, in the LTE network, the uplink resource reserved for PRACH has a bandwidth corresponding to six resource blocks (1.08 MHz), and the PRACH is repeated with a periodicity varies between every 1 to 20 ms [4, 13]. During the PRACH duration, each active IoT device will transmit a preamble to its associated BS to request uplink channel resources for packets transmission. Here, the active IoT device represents that

an IoT device is with non-empty buffers (i.e., $N_{New}^m + N_{Cum}^m > 0$, where N_{New}^m is the number of new arrived packets, and N_{Cum}^m is the number of accumulated packets) and without access restriction, which will be detailed in the following section.

Without loss of generality, we assume the size of buffer in each IoT device is infinite, and none of the packets will be dropped off. At the beginning of the PRACH in the mth time slot, each IoT device checks its buffer status to determine whether itself requires to attempt RACH as shown in the Fig. 1. In detail, the buffer status (i.e., queuing packets) are determined by the new arrived packets, and the accumulated packets that unsuccessfully departs (i.e., unsuccessfully RACH attempts or never been scheduled) before the last time slot.

Once a RACH succeeds, the IoT device will transmit the corresponding data sequences with the scheduled uplink channel resources. Here, we interchangeably use packet to represent the data sequences. In each device, the packets are line a queue waiting to be transmitted, where each packet has the same priority, and the BSs are unaware of the queue status of their associated IoT devices. It is assumed that the BS will only schedule uplink channel resources for the head-of-line packet[2] and each IoT deivce transmits packets via a First Come First Serve (FCFS) packets scheduling scheme - the basic and the most simplest packet scheduling scheme, where all packets are treated equally by placing them at the end of the queue once they arrive [43].

TABLE I: Packets Evolution in the Typical IoT Device.

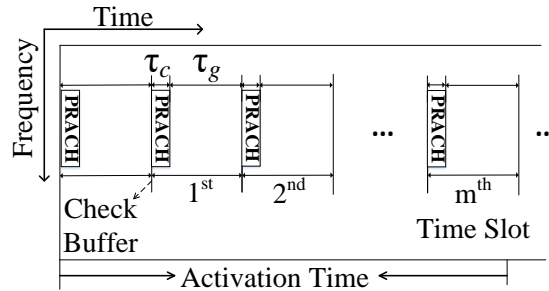| Time Slot	Success	Failure
1st	$N_{Cum}^1 = 0$	$N_{Cum}^1 = 0$
2nd	$N_{Cum}^2 = N_{New}^1 - 1$	$N_{Cum}^2 = N_{New}^1$
3rd	$N_{Cum}^3 = N_{Cum}^2 + N_{New}^2 - 1$	$N_{Cum}^3 = N_{Cum}^2 + N_{New}^2$
$\vdots$	$\vdots$	$\vdots$
mth	$N_{Cum}^m = N_{Cum}^{m-1} + N_{New}^{m-1} - 1$	$N_{Cum}^m = N_{Cum}^{m-1} + N_{New}^{m-1}$

Fig. 1: RACH duration and gap duration, and recording the number of accumulated packets N_{Cum}^m in each time slot.

We model the new arrived packets (N_{New}^m) in the mth time slot at each IoT device as independent Poisson arrival process, Λ_{New}^m with the same intensity ε_{New}^m as [15, 35, 36] (i.e., these new packets are actually arrived within the $(m-1)$th time slot, but they are first considered in the

mth time slot due to the slotted-Aloha behaviour). Therefore, the number of new arrival packets N_{New}^m in a specific time slot (i.e., within the time duration $\tau_c + \tau_g$) is described by the Poisson distribution with $N_{\mathrm{New}}^m \sim \mathrm{Pois}(\mu_{\mathrm{New}}^m)$, where $\mu_{\mathrm{New}}^m = (\tau_c + \tau_g)\varepsilon_{\mathrm{New}}^m$. The accumulated packets (N_{Cum}^m) at each IoT device is evolved following transmission condition over time, which is described in Table I. Specifically, a packet is removed from the buffer once the RACH succeeds, otherwise, this packet will be still in the first place of the queue, and the IoT device will try to request channel resources for the packet in the next available RACH. Note that the data transmission after a successful RACH can be easily extended following the analysis of preamble transmission success probability in RACH. Due to the main focus of this paper is analyzing the contention-based RACH in the mIoT network, we assume that the actual intended packet transmission is always successful if the corresponding RACH succeeds.

D. Transmission Schemes

In the cellular-based mIoT network, a huge number of IoT devices are expected to request for access frequently, such that network congestion may occur due to mass concurrent data and signaling transmission [5]. This network congestion can lead to a low preamble transmission success probability, and thus result in a great number of packets accumulated in buffers, which may cause unexpected delays. A possible solution is to restrict the access attempts in each IoT device according to some RACH control mechanisms. However, the efficiency of these RACH control mechanisms are required to be studied, due to that overly restricting access requests also creates unacceptable delay as well as leads to low channel resource utilization. In this paper, we study the following three schemes:

- **Baseline scheme**: each IoT device attempt RACH immediately when there exists packet in the buffer. The baseline scheme is the simplest scheme without any control of traffic. Due to RACH attempts are not be alleviated at the IoT devices, the baseline scheme can contribute to the relatively faster buffer flushing in non-overloaded network scenarios. However, once the network is overloaded, high delays and service unavailability appear due to mass simultaneous access request.

- **ACB scheme**: each non-empty IoT device draws a random number $q \in [0, 1]$, and attempts to RACH only when $q \leq \mathrm{P}_{\mathrm{ACB}}$, here $\mathrm{P}_{\mathrm{ACB}}$ is the ACB factor specified by the BS according to the network condition [5, 13]. ACB scheme is a basic congestion control method that reduces RACH attempts from the side of IoT devices based on the ACB factor. It is known

that a suitable ACB factor can keep the allowable access in a reasonable density, and assure a relative high data transmission rate when the network is overloaded.

- **Back-off scheme**: each non-empty IoT device transmits packets same as baseline scheme, when there exists packet in the buffer. However, when RACH fails, the IoT device automatically defers the RACH re-attempt and waits for t_{BO} (i.e., the BO facor specified by the BS) time slots until it trys again. Back-off scheme is another basic congestion control method, where each IoT device can automatically alleviate congestion and requires less control message from BS than that of ACB scheme [3].

E. Signal to Noise plus Interference Ratio

As we mentioned earlier, each IoT device transmits a randomly chosen preamble to its associated BS to request for channel resources, where different preambles represent orthogonal sub-channels, and thus only IoT devices choosing same preamble have correlations. Note that IoT devices belonging to a same BS may choose same preamble, such that the intra-cell interference is considered. A preamble can be successfully received at the associated BS, if its SINR is above the threshold. Based on Slivnyak's theorem [44], we formulate the SINR of a typical BS located at the origin as

$$
\begin{aligned}
SINR^m &= \frac{\rho h_0}{\mathcal{I}_{\text{intra}} + \mathcal{I}_{\text{inter}} + \sigma^2} \\
&= \frac{\rho h_0}{\underbrace{\sum_{u_j \in \mathcal{Z}_{\text{in}}} \mathbb{1}_{\{N^m_{\text{New}_j} + N^m_{\text{Cum}_j} > 0\}} \mathbb{1}_{\{UR\}} \rho h_j}_{\mathcal{I}_{\text{intra}}} + \underbrace{\sum_{u_i \in \mathcal{Z}_{\text{out}}} \mathbb{1}_{\{N^m_{\text{New}_i} + N^m_{\text{Cum}_i} > 0\}} \mathbb{1}_{\{UR\}} P_i h_i \|u_i\|^{-\alpha}}_{\mathcal{I}_{\text{inter}}} + \sigma^2},
\end{aligned}
$$

(1)

where ρ is the full path-loss inversion power control threshold, h_0 is the channel power gain from the typical IoT device to its associated BS, σ^2 is the noise power, $\mathcal{I}_{\text{intra}}$ is the aggregate intra-cell interference, $\mathcal{I}_{\text{inter}}$ is the aggregate inter-cell interference[2], $\mathcal{Z}_{in}$ is the set of intra-cell interfering IoT devices, $N^m_{\text{New}_j}$ is the number of new arrived packets of jth device in the mth time slot, $N^m_{\text{Cum}_j}$ is the number of accumulated packets of jth device in the buffer in the mth time slot, $\mathcal{Z}_{out}$ is the set of inter-cell interfering IoT devices, $\|\cdot\|$ is the Euclidean norm, h_i is

---

[2]The PRACH root sequence planning is used to mitigate inter-cell interference among neighboring BS (i.e., neighboring BSs should be using different roots to generate preambles) [13]. However, as [34, 42], we focus on providing a general analytical framework of mIoT network without using PRACH root sequence planning, and the extension taking into account PRACH root sequence planning can be treated in future works.

channel power gain from the ith inter-cell interfering IoT device to the typical BS, u_i is the distance between the ith inter-cell IoT device and the typical BS, and P_i is the actual transmit power of the ith inter-cell IoT device, and P_i depends on the power control threshold ρ and the distance between the ith inter-cell typical IoT device and its associated BS r_i with $P_i = \rho r_i^\alpha$.

In (1), $\mathbb{1}_{\{\cdot\}}$ is the indicator function that takes the value 1 if the statement $\mathbb{1}_{\{\cdot\}}$ is true, and zero otherwise. Whether an IoT device generates interference depends on two conditions: 1) $\mathbb{1}_{\{N_{\text{New}}^m + N_{\text{Cum}_i}^m > 0\}}$, which means that an IoT devices is able to generate interference only when its buffer is non-empty; 2) $\mathbb{1}_{\{UR\}}$, which means that an IoT devices is able to generate interference only when the IoT devices does not defer its access attempt due to RACH scheme. Additionally, once the two conditions are satisfied, we call the IoT device is active.

Mathematically, the non-empty probability of each IoT device can be treated using the thinning process. We assume that the non-empty probability $\mathcal{T}^m$ and the non-restrict probability $\mathcal{R}^m$ of each IoT device in the mth time slot are defined as

$$\mathcal{T}^m = \mathbb{P}\{N_{\text{New}}^m + N_{\text{Cum}}^m > 0\} \text{ ,and } \mathcal{R}^m = \mathbb{P}\{unrestricted\} \tag{2}$$

where the non-restrict probability $\mathcal{R}^m$ depends on the RACH schemes, which will be discussed in the following. The main notations of this paper are summarized in Table II.

TABLE II: Notation Table

Notations	Physical means	Notations	Physical means
λ_D	The intensity of IoT devices	λ_B	The intensity of BSs
ξ	The number of available preambles are reserved for the contention-based RA *	λ_{Dp}	The average intensity of IoT devices using the same preamble
r	The distance	α	The path-loss exponent
h	The Rayleigh fading channel power gain	P	The transmit power *
ρ	The full path-loss power control threshold *	σ^2	The noise power
γ_{th}	The received SINR threshold *	$\mathcal{I}_{\text{intra}}$	The aggregate intra-cell interference
$\mathcal{I}_{\text{inter}}$	The aggregate inter-cell interference	ε_{New}	The intensity of new arrival packets
τ_g	The gap interval duration between two RAs *	τ_c	The duration of PRACH
c	$c = 3.575$ is a constant	m	The time slot
μ_{Cum}^m	The intensity of accumulated packets in the mth time slot	μ_{New}^m	The intensity of new arrival packets in the mth time slot
$\mathcal{T}^m$	The non-empty probability of each IoT device in the mth time slot	$\mathcal{R}^m$	The non-restrict probability of each IoT device in the mth time slot
Z_D	The number of active interfering IoT devices in the cell that a randomly chosen IoT device belongs to	Z_B	The number of active interfering IoT devices in a randomly chosen cell
N_{New}^m	The number new arrived packets in the mth time slot in a specific IoT device	N_{Cum}^m	The number accumulated packets in the mth time slot in a specific IoT device
P_{ACB}	The ACB factor with the ACB scheme *	t_{BO}	The BO factor with the BO scheme *
Remarks	The variables marked with * are configurable parameters.		

III. SINR Analysis

In this section, we provide a general framework for the performance analysis of each single time slot and each RACH scheme. Due to that the preamble has an equal probability to be chosen, the analysis performed on a randomly chosen preamble can represent the whole network. The probability that the received SINR at the BS exceeds a certain threshold γ_{th} is written as

$$
\begin{aligned}
\mathbb{P}\Big\{\frac{\rho h_o}{\mathcal{I}_{\text{inter}} + \mathcal{I}_{\text{intra}} + \sigma^2} \geq \gamma_{\text{th}}\Big\} &= \mathbb{P}\Big\{h_o \geq \frac{\gamma_{\text{th}}}{\rho}(\mathcal{I}_{\text{inter}} + \mathcal{I}_{\text{intra}} + \sigma^2)\Big\} \\
&= \mathbb{E}\Big[\exp\Big\{-\frac{\gamma_{\text{th}}}{\rho}(\mathcal{I}_{\text{inter}} + \mathcal{I}_{\text{intra}} + \sigma^2)\Big\}\Big] \\
&= \exp\big(-\frac{\gamma_{\text{th}}}{\rho}\sigma^2\big)\mathcal{L}_{\mathcal{I}_{\text{intra}}}\big(\frac{\gamma_{\text{th}}}{\rho}\big)\mathcal{L}_{\mathcal{I}_{\text{inter}}}\big(\frac{\gamma_{\text{th}}}{\rho}\big),
\end{aligned} \tag{3}
$$

where $\mathcal{L}_{\mathcal{I}}(\cdot)$ denotes the Laplace Transform of the PDF of the aggregate interference $\mathcal{I}$. The Laplace Transform of aggregate inter-cell interference is characterized in the following Lemma.

Lemma 1. *The Laplace Transform of aggregate inter-cell interference received at the typical BS in the cellular-based mIoT network is given by*

$$
\mathcal{L}_{\mathcal{I}_{\text{inter}}}\big(\frac{\gamma_{\text{th}}}{\rho}\big) = \exp\Big(-2(\gamma_{\text{th}})^{\frac{2}{\alpha}}\frac{\mathcal{T}^m \mathcal{R}^m \lambda_{Dp}}{\lambda_B}\int_{(\gamma_{\text{th}})^{\frac{-1}{\alpha}}}^{\infty}\frac{y}{1+y^\alpha}dy\Big), \tag{4}
$$

where $\mathcal{T}^m$ and $\mathcal{R}^m$ are defined in (2). Remind that λ_{Dp} is the intensity of IoT devices using same preamble.

Proof. See Appendix A. □

We perform the analysis on a randomly chosen BS and a BS associating with a randomly chosen IoT device in terms of the preamble detection probability and the preamble transmission success probability. The probability that the received SINR at a randomly chosen BS exceeds a certain threshold γ_{th} has been studied in many stochastic geometry works [23, 30, 37]. Those analyses focus on the uplink transmission channel of a cellular networks, without considering intra-cell interference due to TDMA or FDMA assumptions, and only considered inter-cell interference. In their models, the average aggregate interference is the same, no matter if the tagged BS is randomly chosen, or is determined by a randomly chosen device via association, thus the probability that the received SINR exceeds a threshold γ_{th} at a randomly chosen BS is equally same as the probability of a BS associating with a randomly chosen uplink device.

Different from the conventional stochastic geometry works in [23, 25, 30, 37] with no intra-cell interference, we take into account the intra-cell interference due to the same preamble reuse among many IoT devices in a cell during their uplink RACH. We will derive the preamble

detection probability from the view of a *randomly chosen BS* (i.e., each BS has an equal probability to be chosen), and the preamble transmission success probability from the view of a BS that a *randomly chosen IoT device* belongs to (i.e., the probability of a BS being chosen is determined by the number of its associated IoT devices). An example is shown in Fig. 2 to make a distinction between these two characteristics. For the preamble detection probability, each BS has equal probability to be chosen, and for the preamble transmission success probability, the BS 1 has a probability of 5/6 to be chosen (i.e., BS 1 covers 5 IoT devices), but BS 2 only has a probability of 1/6 to be chsoen. Concludely, the difference between these two characteristics comes from the fact that a cell, that a *randomly chosen IoT device* belonging to, has chance to cover more IoT devices than a *randomly chosen cell* [25, 45].
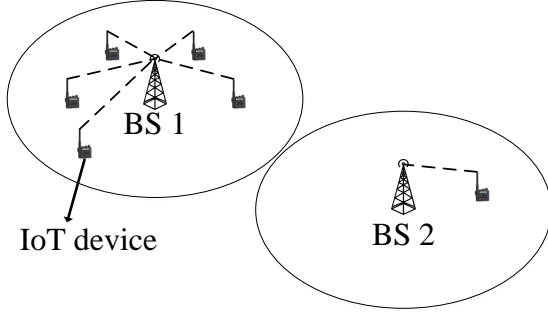

Fig. 2: An example of network model shows differences between the preamble detection probability and the preamble transmission success probability.
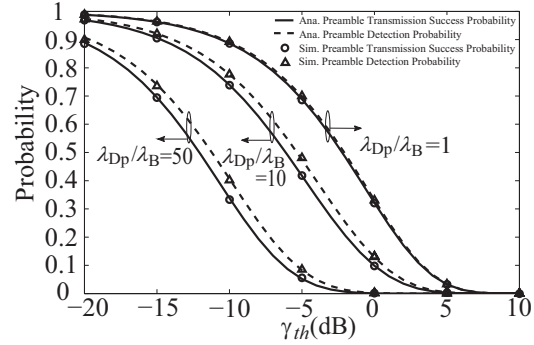

Fig. 3: The preamble detection probability $\mathcal{P}^1_{detection}$ and the preamble transmission success probability $\mathcal{P}^1$ versus the SINR threshold γ_{th} for the 1st single time slot. We set $\mathcal{T}^1 = 1 - e^{0.1}$, $\rho = -90$ dBm, $\sigma^2 = -90$ dBm, $\lambda_B = 10$ BS/km^2, $\alpha = 4$, $\gamma_{th} = -10$ dB, and the baseline scheme is considered with $\mathcal{R}^1 = 1$.

A. Preamble Transmission Success Probability

We first perform analysis on a BS in which a randomly chosen IoT device belongs to, where the other active IoT devices in the same cell choosing same preamble are visualized as interfering IoT devices. Since the interference generating by each intra-cell IoT device is strictly equal to ρ, such that the aggregate intra-cell interference only depends on the number of active interfering IoT devices in the Voronoi cell. We assume $\widehat{Z}_{in}$ denotes the number of active IoT device in a specific Voronoi cell, and let $Z_D = \left| \widehat{Z}_{in} \right| - 1$ denotes the number of active interfering IoT devices in such cell, where the Laplace Transform of aggregate intra-cell interference is conditioned on Z_D. The Probability Density Function (PDF) of the number of active interfering IoT devices

in a Voronoi cell has been derived by the Monte Carlo method in [46], and conditioned on a randomly chosen IoT device in its cell, the PMF of the number of interfering intra-cell IoT devices in that cell Z_D is expressed as [25]

$$\mathbb{P}\{Z_D = n\} = \frac{c^{(c+1)}\Gamma(n+c+1)(\frac{\mathcal{T}^m\mathcal{R}^m\lambda_{Dp}}{\lambda_B})^n}{\Gamma(c+1)\Gamma(n+1)(\frac{\mathcal{T}^m\mathcal{R}^m\lambda_{Dp}}{\lambda_B}+c)^{n+c+1}}, \tag{5}$$

where $c = 3.575$ is a constant related to the approximate PMF of the PPP Voronoi cell, and $\Gamma(\cdot)$ is gamma function. The Laplace Transform of aggregate intra-cell interference is conditioned on the number of interfering intra-cell IoT devices Z_D, which is derived in the following Lemma.

Lemma 2. *The Laplace Transform of aggregate intra-cell interference at the BS to which a randomly chosen IoT device belongs in the cellular-based mIoT network is given by*

$$\mathcal{L}_{\mathcal{I}_{\text{intra}}}(\frac{\gamma_{\text{th}}}{\rho}) = \mathbb{P}\{Z_D = 0\} + \sum_{n=1}^{\infty}\mathbb{P}\{Z_D = n\}\left(\frac{1}{1+\gamma_{\text{th}}}\right)^n = \left(1 + \frac{\mathcal{T}^m\mathcal{R}^m\lambda_{Dp}\gamma_{\text{th}}}{c\lambda_B(1+\gamma_{\text{th}})}\right)^{-c-1}. \tag{6}$$

Proof. See Appendix B. $\qquad\qquad\square$

Substituting (4) and (6) into (3), we derive the preamble transmission success probability of the 1st time slot P_t^1 in the following theorem.

Theorem 1. *In the depicted cellular-based mIoT network, the preamble transmission success probability of a randomly chosen IoT device of the mst time slot is given by*

$$\mathcal{P}^m = \exp\left(-\frac{\gamma_{\text{th}}\sigma^2}{\rho} - 2(\gamma_{\text{th}})^{\frac{2}{\alpha}}\frac{\mathcal{T}^m\mathcal{R}^m\lambda_{Dp}}{\lambda_B}\int_{(\gamma_{\text{th}})^{\frac{-1}{\alpha}}}^{\infty}\frac{y}{1+y^{\alpha}}dy\right)\left(1 + \frac{\mathcal{T}^m\mathcal{R}^m\lambda_{Dp}\gamma_{\text{th}}}{c\lambda_B(1+\gamma_{\text{th}})}\right)^{-c-1}. \tag{7}$$

Proof. See Appendix A and B. $\qquad\qquad\square$

B. Preamble Detection Probability

Next, we move to the preamble decoding probability that is performed on a randomly chosen BS, and one of its active associated IoT device (with a preamble being randomly chosen) is tagged, where the other active IoT devices choosing same preamble are visualized as interfering IoT devices. Conditioned on a randomly chosen BS, the Probability Mass function (PMF) of the number of IoT devices $\left|\widehat{Z}_{in}\right|$ in a randomly chosen BS has been clearly introduced in [25], which is expressed as

$$\mathbb{P}\left\{\left|\widehat{Z}_{in}\right| = n\right\} = \frac{c^c\Gamma(n+c)(\frac{\mathcal{T}^m\mathcal{R}^m\lambda_{Dp}}{\lambda_B})^n}{\Gamma(c)\Gamma(n+1)(\frac{\mathcal{T}^m\mathcal{R}^m\lambda_{Dp}}{\lambda_B}+c)^{n+c}}. \tag{8}$$

For the Voronoi cell with at least one active IoT device, the PMF of the number of active interfering intra-cell IoT devices Z_B in a randomly chosen Voronoi cell (BS) is given by

$$\mathbb{P}\left\{Z_B = n\right\} = \frac{\mathbb{P}\left\{\left|\widehat{Z}_{in}\right| = n+1\right\}}{1 - \mathbb{P}\left\{\left|\widehat{Z}_{in}\right| = 0\right\}} = \frac{c^c \Gamma(n+c+1)(\frac{\mathcal{T}^m \mathcal{R}^m \lambda_{Dp}}{\lambda_B})^{(n+1)}(1 + \frac{\mathcal{T}^m \mathcal{R}^m \lambda_{Dp}}{c\lambda_B})^c}{\Gamma(c)\Gamma(n+2)(\frac{\mathcal{T}^m \mathcal{R}^m \lambda_{Dp}}{\lambda_B} + c)^{n+c+1}\left((1 + \frac{\mathcal{T}^m \mathcal{R}^m \lambda_{Dp}}{c\lambda_B})^c - 1\right)}. \tag{9}$$

The difference between (9) and (5) is clearly explained in [45]. Briefly speaking, in (9), each Voronoi cell has an equal probability to be chosen, whilst in (5), a Voronoi cell with more IoT devices has a higher probability to be chosen. Following similar approach in the proof of Lemma 2, and with the help of (9), we derive the preamble detection probability of the typical BS in the 1st time slot $\mathcal{P}^m_{detection}$ in the following Lemma.

Lemma 3. *The preamble detection probability of an typical IoT device located in a randomly chosen BS in the cellular-based mIoT network is given by*

$$\mathcal{P}^m_{detection} = \exp\left(-\frac{\gamma_{th}\sigma^2}{\rho} - 2(\gamma_{th})^{\frac{2}{\alpha}}\frac{\mathcal{T}^m \mathcal{R}^m \lambda_{Dp}}{\lambda_B}\int_{(\gamma_{th})^{\frac{-1}{\alpha}}}^{\infty}\frac{y}{1+y^\alpha}dy\right)\left[\left(1 + \frac{\mathcal{T}^m \mathcal{R}^m \lambda_{Dp}\gamma_{th}}{c\lambda_B(1+\gamma_{th})}\right)^{-c}\right.$$
$$\left. - \left(\frac{c\lambda_B}{c\lambda_B + \mathcal{T}^m \mathcal{R}^m \lambda_{Dp}}\right)^{-c}\right]\frac{(1+\gamma_{th})(1+(\mathcal{T}^m \mathcal{R}^m \lambda_{Dp}/\lambda_B))^c}{(1+(\mathcal{T}^m \mathcal{R}^m \lambda_{Dp}/\lambda_B))^c - 1}. \tag{10}$$

Proof. Following the proofs of Lemma 1 and Lemma 2. $\qquad\square$

In Lemma 3, the preamble detection probability of an IoT device located in a *randomly chosen BS* is analyzed based on the number of active interfering intra-cell IoT devices in that randomly chosen Voronoi cell (BS) in (9), whereas in Theorem 1, the preamble transmission success probability of a *randomly chosen IoT device* is described by the number of interfering intra-cell IoT devices in that cell, where that randomly chosen IoT device belongs to in (5). Fig. 3 plots the preamble detection probability $\mathcal{P}_{detection}$ and the preamble transmission success probability $\mathcal{P}$ versus the SINR threshold γ_{th} for a single time slot using (10) and (7), respectively. As expected, the preamble transmission success probability of a randomly chosen IoT device is always lower than the preamble detection probability of a randomly chosen BS, due to that a randomly chosen IoT device has higher chance to associate with a BS with large number of intra-cell interfering IoT devices as shown in (9) and (5), which leads to relatively low average received SINR.

In the following queue evolution analysis, we will study each packet that departs or accumulates at each IoT device in each time slot, which is determined by whether the RACH procedure succeeds or fails. To do so, the probability of RACH success in each time slot is required

under the condition that each IoT device is equally treated (i.e., each IoT device has an equal probability to be chosen as a typical device no matter it is located in a cell with a relatively large or small number of IoT devices). Therefore, the following derivations are all based on the preamble transmission success probability $\mathcal{P}^m$ (i.e. it is performed on a BS in which a randomly chosen IoT device belongs to.) provided in Theorem 1.

IV. QUEUE EVOLUTION ANALYSIS

In this section, we analyze the performance of the cellular-based mIoT network in each time slot with different schemes. As mentioned in (7), the preamble transmission success probability depends on the non-empty probability $\mathcal{T}^m$ and the non-restrict probability $\mathcal{R}^m$ of each IoT device, which raises the problem how to study the queue status of each IoT device in each time slot.

The queue status and the preamble transmission are interdependent, and imposes a causality problem. More specifically, the preamble transmission of a typical IoT device in the current time slot depends on the aggregate interference from those active IoT devices in that time slot, thus we need to know the current queue status, which is decided by the previous queue statuses, as well as the preamble transmission success probabilities of previous time slots. Recall that the evolution of queue status follows Table I, where the accumulated packets come from the packets that are not successfully transmitted in the previous time slots.

Mathematically, to derive the preamble transmission success probability of an randomly chosen IoT device in the mth time slot $\mathcal{P}^m$, we first derive the non-empty probability $\mathcal{T}^m$ and the non-restrict probability $\mathcal{R}^m$ of the IoT device, which are decided by $\mathcal{P}^{m-1}$, $\mathcal{T}^{m-1}$, and $\mathcal{R}^{m-1}$. As the number and locations of BSs and IoT devices are fixed all time once they are deployed, the locations of active IoT devices are slightly correlated across time. However, this correlation only has very little impact on the distributions of active IoT devices, and thus we approximate the distributions of non-empty IoT devices following independent PPPs in each time slot. In the rest of this section, we first describe the general analytical framework used to derive the the non-empty probability $\mathcal{T}^m$ in each time slot, and then delve into the analysis details of the non-restrict probability $\mathcal{R}^m$ in each time slot for each RACH scheme.

A. Non-Empty Probability $\mathcal{T}^m$

In the 1st time slot, the number of packets in an IoT device only depends on the new packets arrival process Λ_{New}^1, such that the non-empty probability of each IoT device $\mathcal{T}^1$ in the 1st time

slot is expressed as

$$\mathcal{T}^1 = \mathbb{P}\{N_{\text{New}}^1 > 0\} = 1 - e^{-\mu_{\text{New}}^1}, \tag{11}$$

where μ_{New}^1 is the intensity of new arrival packets. Note that the non-restrict probability in the 1st time slot $\mathcal{R}^1 = 1$ with the baseline scheme, and for other RACH schemes, $\mathcal{R}^1$ is determined by their transmission policies, which will be detailed in the following subsection. Substituting (11) and $\mathcal{R}^1$ into (7), we derive the preamble transmission success probability of a randomly chosen IoT device in the 1st time slot $\mathcal{P}^1$.

Next, we derive the non-empty probability and the preamble transmission success probability of a randomly chosen IoT device in the mth time slot in the following Theorem.

Theorem 2. *The accumulated packets number of an IoT device in any time slot should be approximately Poisson distributed. As such, we approximate the number of accumulated packets in the mth time slot N_{Cum}^m as Poisson distribution Λ_{Cum}^m with intensity μ_{Cum}^m. The intensity of accumulated packets μ_{Cum}^m $(m > 1)$ in the mth time slot is derived as*

$$\mu_{\text{Cum}}^m = \mu_{\text{New}}^{m-1} + \mu_{\text{Cum}}^{m-1} - \mathcal{R}^{m-1}\mathcal{P}^{m-1}\big(1 - e^{-\mu_{\text{New}}^{m-1} - \mu_{\text{Cum}}^{m-1}}\big). \tag{12}$$

The non-empty probability of each IoT device in the mth time slot is derived as

$$\mathcal{T}^m = 1 - e^{-\mu_{\text{New}}^m - \mu_{\text{Cum}}^m}. \tag{13}$$

Substituting $\mathcal{T}^m$ and $\mathcal{R}^m$ into (7), we derive the preamble transmission success probability of a randomly chosen IoT device in the mth time slot $\mathcal{P}^m$. Note that $\mathcal{R}^m = 1$ with the baseline scheme, and for other RACH schemes, $\mathcal{R}^m$ are determined by their transmission policies, which will be detailed in the following subsection[3].

Proof. We first derive the non-empty probability in each time slot using exact probabilistic statistics. In the 2nd time slot, the PMF of the accumulated packets N_{Cum}^2 is expressed as

$$f_{N_{\text{Cum}}^2}(x) = \begin{cases} e^{-\mu_{\text{New}}^1} + \mu_{\text{New}}^1 e^{-\mu_{\text{New}}^1}\mathcal{R}^1\mathcal{P}^1, & x = 0, \\ \dfrac{(\mu_{\text{New}}^1)^x e^{-\mu_{\text{New}}^1}}{x!}(1 - \mathcal{R}^1\mathcal{P}^1) + \dfrac{(\mu_{\text{New}}^1)^{x+1} e^{-\mu_{\text{New}}^1}}{(x+1)!}\mathcal{R}^1\mathcal{P}^1, & x > 0. \end{cases} \tag{14}$$

The reason for (14) is that the number of accumulated packets in the 2nd time slot equals to x occurs only when 1) the number of accumulated packets in the 1st time slot equals to $x + 1$, and one packet is successfully transmitted in the 1st time slot, and 2) the number of accumulated

---

[3]With minor modification, this theorem can also be leveraged to study other traffic models, such as the time limited Uniform Distribution and the time limited Beta distribution [5].

packets in the 1st time slot equals to x, and no packet is successfully transmitted in the 1st time slot.

Based on (14), we derive the CDF of the number of accumulated packets in the 2nd time slot N_{Cum}^2 as

$$F_{N_{\mathrm{Cum}}^2}(y) = \sum_{x=0}^{y} f_{N_{\mathrm{Cum}}^2}(x) = \frac{(\mu_{\mathrm{New}}^1)^{y+1} e^{-\mu_{\mathrm{New}}^1}}{(y+1)!} \mathcal{R}^1 \mathcal{P}^1 + \sum_{x=0}^{y} \frac{(\mu_{\mathrm{New}}^1)^x e^{-\mu_{\mathrm{New}}^1}}{x!}. \quad (15)$$

We are interested in the zero-accumulated packets probability in the 2nd time slot, since it determines the density of non-empty IoT devices (with more than one packet in the buffer) in that time slot, and the activity probability of IoT devices. Based on the probabilistic statistics and (14), we present the non-empty probability of IoT devices in the $2nd$ time slot as

$$\mathcal{T}_{\mathrm{BL}}^2 = 1 - e^{-\mu_{\mathrm{New}}^2} \left(e^{-\mu_{\mathrm{New}}^1} + \mu_{\mathrm{New}}^1 e^{-\mu_{\mathrm{New}}^1} \mathcal{R}^1 \mathcal{P}^1 \right). \quad (16)$$

Substituting (16) and $\mathcal{R}^2 = 1$ into (7), we derive the preamble transmission success probability of a randomly chosen IoT device in the 2nd time slot $\mathcal{P}^2$.

Similar as (14) and (15), we can derive the PMF and the CDF of the number of accumulated packets in the 3rd time slot N_{Cum}^3 as

$$f_{N_{\mathrm{Cum}}^3}(x) = $$
$$\begin{cases} e^{-\mu_{\mathrm{New}}^2} f_{N_{\mathrm{Cum}}^2}(0) + \mathcal{R}^2 \mathcal{P}^2 \left[\mu_{New}^2 e^{-\mu_{\mathrm{New}}^2} f_{N_{\mathrm{Cum}}^2}(0) + e^{-\mu_{\mathrm{New}}^2} f_{N_{\mathrm{Cum}}^2}(1) \right], & x = 0, \\ (1 - \mathcal{R}^2 \mathcal{P}^2) \sum_{z=0}^{x} \left[\frac{(\mu_{\mathrm{New}}^2)^z e^{-\mu_{\mathrm{New}}^2}}{(z)!} f_{N_{\mathrm{Cum}}^2}(x-z) \right] & \\ + \mathcal{R}^2 \mathcal{P}^2 \sum_{z=0}^{x+1} \left[\frac{(\mu_{\mathrm{New}}^2)^z e^{-\mu_{\mathrm{New}}^2}}{(z)!} f_{N_{\mathrm{Cum}}^2}(x+1-z) \right], & x > 0, \end{cases} \quad (17)$$

and

$$F_{N_{\mathrm{Cum}}^3}(y) = \mathcal{R}^2 \mathcal{P}^2 \sum_{z=0}^{y+1} \left[\frac{(\mu_{\mathrm{New}}^2)^z e^{-\mu_{\mathrm{New}}^2}}{(z)!} f_{N_{\mathrm{Cum}}^2}(y+1-z) \right] + \sum_{x=0}^{y} \sum_{z=0}^{x} \left[\frac{(\mu_{\mathrm{New}}^2)^z e^{-\mu_{\mathrm{New}}^2}}{(z)!} f_{N_{\mathrm{Cum}}^2}(x-z) \right], \quad (18)$$

respectively. In (17) and (18), $f_{N_{\mathrm{Cum}}^2}(x)$ is given in (14). Generally, the PMF and CDF of N_{Cum}^m in the mth time slot can be derived by the iteration process.

However, as m increases, the complexity of these derivations exponentially increases, and thus they become hard to analyze. Due to the new packets arrival at each IoT device is modeled by independent Poisson process, the packets departure can be treated as an approximated thinning process (i.e., the thinning factor is a function relating to the preamble transmission success probability, the non-empty probability, and the non-restrict probability) of the arrived packets.

Therefore, after this thinning process in a specific time slot, the least packets (i.e. the accumulated packets) number at each IoT device can be approximated as Poisson distribution with the same mean. As such, we approximate the number of accumulated packets in the mth time slot N_{Cum}^m as Poisson distribution Λ_{Cum}^m with intensity μ_{Cum}^m. The intensity of accumulated packets μ_{Cum}^m ($m > 1$) in the mth time slot is derived as

As such, we approximate the number of accumulated packets in the mth time slot as a Poisson distribution ($m > 1$), where the number of accumulated packets of an IoT device in the mth time slot N_{Cum}^m is approximated as Poisson distribution Λ_{Cum}^m with intensity μ_{Cum}^m. In the 2nd time slot, μ_{Cum}^2 depends on the new packets arrival rate μ_{New}^1 and the preamble transmission success probability $\mathcal{P}^1$ of an IoT device in the 1st time slot, which is given by

$$\mu_{\text{Cum}}^2 = \underbrace{\mathcal{R}^1 \mathcal{P}^1 \Big(\sum_{x=1}^{\infty} f_{N_{\text{New}}^1}(x) \cdot (x-1) \Big)}_{(a)} + \underbrace{\big((1-\mathcal{R}^1) + \mathcal{R}^1(1-\mathcal{P}^1) \big) \Big(\sum_{x=1}^{\infty} f_{N_{\text{New}}^1}(x) \cdot x \Big)}_{(b)}$$

$$= \mathcal{R}^1 \mathcal{P}^1 \Big(\sum_{x=1}^{\infty} \frac{(\mu_{\text{New}}^1)^x e^{-\mu_{\text{New}}^1}(x-1)}{x!} \Big) + (1-\mathcal{R}^1\mathcal{P}^1)\mu_{\text{New}}^1$$

$$= \mathcal{R}^1 \mathcal{P}^1 \Big(\sum_{x=0}^{\infty} \frac{(\mu_{\text{New}}^1)^x e^{-\mu_{\text{New}}^1} x}{x!} - \sum_{x=1}^{\infty} \frac{(\mu_{\text{New}}^1)^x e^{-\mu_{\text{New}}^1}}{x!} \Big) + (1-\mathcal{R}^1\mathcal{P}^1)\mu_{\text{New}}^1$$

$$= \mu_{\text{New}}^1 - \mathcal{R}^1 \mathcal{P}^1 \big(1 - e^{-\mu_{\text{New}}^1}\big), \tag{19}$$

where $\mu_{\text{New}}^1 = (\tau_c + \tau_g)\varepsilon_{\text{New}}^1$, $\varepsilon_{\text{New}}^1$ is the new packets arrival rate of each device in the 1st time slot, $f_{N_{\text{New}}^1}(\cdot)$ is the PMF of the number of new arrived packets N_{New}^1, $\mathcal{P}^1$ is given in (7) of Theorem 1. In (19), (a) is the density of the accumulated packets in the 2nd time slot when a packet is successfully transmitted in the 1st time slot, and (b) is the density of the accumulated packets in the 2nd time slot when the congestion alleviation or the unsuccess transmission occurs in the 1st time slot.

According to Poisson approximation and (19), the CDF of the number of packets in the 2nd time slot due to previous accumulated packets N_{Cum}^2 is approximated as

$$F_{N_{\text{Cum}}^2}(y) \approx \sum_{z=0}^{y} \frac{(\mu_{\text{Cum}}^2)^z e^{-\mu_{\text{Cum}}^2}}{z!} = \sum_{z=0}^{y} \frac{\big(\mu_{\text{New}}^1 - \mathcal{R}^1\mathcal{P}^1\big(1 - e^{-\mu_{\text{New}}^1}\big) \big)^z e^{-\mu_{\text{New}}^1 - \mathcal{R}^1\mathcal{P}^1\big(1 - e^{-\mu_{\text{New}}^1}\big)}}{z!},$$

$$\tag{20}$$

and the non-empty probability of an IoT devices in the 2nd time slot is approximated as

$$\mathcal{T}^2 \approx 1 - e^{-\mu_{\text{New}}^2 - \mu_{\text{Cum}}^2}, \tag{21}$$

where μ_{Cum}^2 is given in (19).

Similarly, the intensity of the number of accumulated packets in the 3rd time slot μ_{Cum}^3 is

$$\mu_{\text{Cum}}^3 = \mu_{\text{New}}^2 + \mu_{\text{Cum}}^2 - \mathcal{R}^2 \mathcal{P}^2 \left(1 - e^{-\mu_{\text{New}}^2 - \mu_{\text{Cum}}^2}\right), \tag{22}$$

where μ_{Cum}^3 is given in (22). Thus, we approximate the CDF of the number of accumulated packets in the 3nd time slot N_{Cum}^3 as

$$F_{N_{\text{Cum}}^3}(y) \approx \sum_{z=0}^{y} \frac{\left(\mu_{\text{Cum}}^3\right)^z e^{-\mu_{\text{Cum}}^3}}{z!}. \tag{23}$$

The intensity of the number of accumulated packets in the mth time slot ($m > 3$) is derived following (19), which is already given in (12). For simplicity, we omit this expression here.
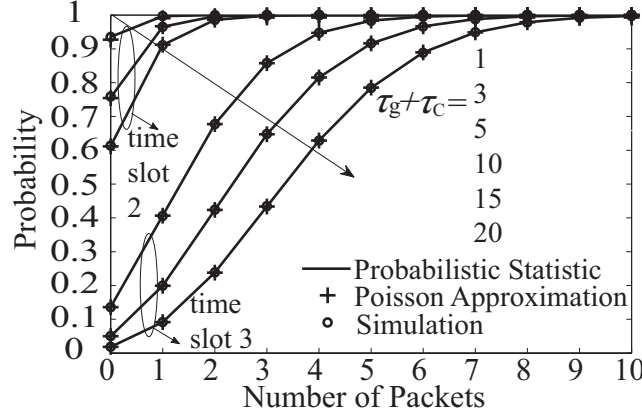

Fig. 4: Comparing the CDFs of the number of accumulated packets between probabilistic statistics and Poisson approximation in the 2nd and the 3rd time slots. We present 6 scenarios with different RACH interval durations, where $(\tau_c + \tau_g) = 1, 3, 5, 10, 15$ and 20 ms. The simulation parameters are $\lambda_B = 10$ BS/km^2, $\lambda_{Dp} = 100$ IoT deivces/preamble/km^2, $\rho = -90$ dBm, $\sigma^2 = -90$ dBm, $\varepsilon_{\text{New}}^1 = \varepsilon_{\text{New}}^2 = \varepsilon_{\text{New}}^3 = 0.1$ packets/ms, and the baseline scheme with $\mathcal{R}^m = 1$.

Fig. 4 shows the CDFs of the number of accumulated packets via simulation, as well as calculating by the probabilistic statistics and the Poisson approximation. We see the close match among the probabilistic statistics, Poisson approximation and the simulation results, which validates our approximation approach. More simulation results will be provided in the Section V to validate the Poisson approximation approach.

□

B. Non-Restrict Probability $\mathcal{R}^m$

1) The Baseline Scheme: The baseline scheme allows each IoT device to attempt RACH immediately when there exists packet in the buffer, and thus the non-restrict probability is always equal to 1 in any time slot ($\mathcal{R}_{\text{BL}}^m = 1$).

2) The ACB Scheme: In the ACB scheme, the BS first broadcasts the ACB factor $\mathrm{P}_{\mathrm{ACB}}$, then each non-empty IoT device draws a random number $q \in [0,1]$, and attempts to RACH only when q smaller than or equal to the ACB factor $\mathrm{P}_{\mathrm{ACB}}$. Therefore, the non-restrict probability is always equal to $\mathrm{P}_{\mathrm{ACB}}$ in any time slot ($\mathcal{R}_{\mathrm{ACB}}^m = \mathrm{P}_{\mathrm{ACB}}$).

3) The Back-Off Scheme: In the back-off scheme, each IoT device defers its access and waits for t_{BO} time slots, when such IoT devices failed to transmit a packet in the last time slot. The analysis of the non-restrict probability with the back-off scheme $\mathcal{R}_{\mathrm{BO}}^m$ is similar to the ACB scheme, due to the back-off procedure can be visualised as a group of IoT devices are completely barred in a specific time slot. In the 1st time slot, none of IoT device defers the access attempt, such that the transmission procedure is same as the baseline scheme ($\mathcal{R}_{\mathrm{BL}}^1 = 1$). After the 1st time slot, the back-off procedure starts to execute, an non-empty IoT device defers its access attempt if the back-off being trigged.

Due to the back-off mechanism, only active IoT devices without RACH attempt failures in the last t_{BO} time slots can attempt to transmit a preamble, and only those IoT devices generate interference that determine the preamble transmission success probability in the mth time slot. The non-restrict probability with the back-off scheme $\mathcal{R}_{\mathrm{BO}}^m$ is derived as

$$
\mathcal{R}_{\mathrm{BO}}^m = \begin{cases} 1, & m = 1, \\ 1 - \Big[\sum_{j=1}^{m-1} \underbrace{(1-\mathcal{P}_{\mathrm{BO}}^j)\mathcal{T}_{\mathrm{BO}}^j \mathcal{R}_{\mathrm{BO}}^j}_{(a)}\Big]\mathcal{T}_{\mathrm{BO}}^m, & (t_{\mathrm{BO}}+1) \geq m > 1, \\ 1 - \Big[\sum_{j=m-t_{\mathrm{BO}}}^{m-1} \underbrace{(1-\mathcal{P}_{\mathrm{BO}}^j)\mathcal{T}_{\mathrm{BO}}^j \mathcal{R}_{\mathrm{BO}}^j}_{(a)}\Big]\mathcal{T}_{\mathrm{BO}}^m, & m > t_{\mathrm{BO}}, \end{cases}
\tag{24}
$$

where (a) is the probability that an randomly chosen IoT device fails to transmit a preamble in the jth time slot, and thus this IoT device would defer its RACH request in the mth time slot due to the back-off mechanism.

V. PERFORMANCE METRICS

We have derived the preamble transmission success probability in each time slot in the last section, and then based on the derived probability, many performance metrics can be obtained.

A. *The Number of Received Packets per BS*

We first analyze the number of received packets per BS of cellular-based mIoT networks as a function of the densities of IoT devices using same preamble and BS, which reflects the density

of successfully RACH IoT devices using same preamble per BS ([25], e.q. (6)). In our model, the number of received packets per BS in the mth time slot $\mathcal{C}^m$ is defined as

$$\mathcal{C}^m \triangleq \mathcal{T}^m \mathcal{R}^m \lambda_{Dp} \cdot \mathcal{P}^m / \lambda_B. \tag{25}$$

Substituting (7) into (25), the number of received packets per BS $\mathcal{C}^m$ is derived as

$$\mathcal{C}^m = \frac{\mathcal{T}^m \mathcal{R}^m \lambda_{Dp}}{\lambda_B} \exp\left(-\frac{\gamma_{\text{th}} \sigma^2}{\rho} - 2(\gamma_{\text{th}})^{\frac{2}{\alpha}} \frac{\mathcal{T}^m \mathcal{R}^m \lambda_{Dp}}{\lambda_B} \int_{(\gamma_{\text{th}})^{\frac{-1}{\alpha}}}^{\infty} \frac{y}{1+y^\alpha} dy\right) \left(1 + \frac{\mathcal{T}^m \mathcal{R}^m \lambda_{Dp} \gamma_{\text{th}}}{c \lambda_B (1 + \gamma_{\text{th}})}\right)^{-c-1}. \tag{26}$$

In (25), $\mathcal{C}^m$ is negatively proportional to the density ratio λ_B, and in (7), the preamble transmission success probability $\mathcal{P}^m$ is positively proportional to the density ratio λ_B, which positively improves $\mathcal{C}^m$. Therefore, λ_B introduce a tradeoff in the system performance of $\mathcal{C}^m$, which is jointly determined by two opposite factors: 1) the average received SINR of each BS, 2) the average number of associated IoT devices of each BS. Practically, when BSs are deployed with a relatively large density, rare IoT devices can successfully transmit a preamble to their associated BSs, due to the large interference leading to extremely low received SINR. In this scenario, $\mathcal{C}^m$ is dominantly determined by the factor 1 (i.e., average received SINR of each BS), and thus increasing the BS intensity λ_B can greatly improve the number of received packets per BS. However, increasing the BS intensity increases the received SINR, but decreases the average number of associated IoT devices, which contributes to higher number of received packets per BS in the scenario of overloaded network, but decreases the that in the scenario of non-overloaded network due to low utilization of channel resources (i.e., the factor 2 dominantly determined $\mathcal{C}^m$ in this scenario). Therefore, $\mathcal{C}^m$ is concave downward, and there exists a optimal BS density deployment which enables the maximum number of received packets per BS as shown in (27).

To obtain the optimal number of received packets per BS in proposed IoT-enabled cellular network, we take the first derivative on C^m, and obtain the density of BSs achieving the maximum number of received packets per BS λ_B^* as

$$\lambda_B^* = \frac{\mathcal{T}^m \mathcal{R}^m \lambda_{Dp}}{2} \left(2(\gamma_{\text{th}})^{\frac{2}{\alpha}} \int_{(\gamma_{\text{th}})^{\frac{-1}{\alpha}}}^{\infty} \frac{y}{1+y^\alpha} dy + \frac{\gamma_{\text{th}}}{(1+\gamma_{\text{th}})} + \right.$$
$$\left. \sqrt{\left(2(\gamma_{\text{th}})^{\frac{2}{\alpha}} \int_{(\gamma_{\text{th}})^{\frac{-1}{\alpha}}}^{\infty} \frac{y}{1+y^\alpha} dy\right)^2 + \frac{\gamma_{\text{th}}^2}{(1+\gamma_{\text{th}})^2} + \left(4 + \frac{8}{c}\right)\left(\int_{(\gamma_{\text{th}})^{\frac{-1}{\alpha}}}^{\infty} \frac{y}{1+y^\alpha} dy\right) \frac{(\gamma_{\text{th}})^{\frac{\alpha+2}{\alpha}}}{(1+\gamma_{\text{th}})}}\right). \tag{27}$$

B. Mean of $\mathcal{C}^m$ and $\mathcal{P}^m$

The number of received packets per BS in the mth time slot $\mathcal{C}^m$ is derived by using $\mathcal{P}^m$ following (26). Next, we derive the mean of preamble transmission success probabilities of a

randomly chosen IoT device over M time slots and the mean of number of received packets per BS over M time slots, which are expressed as

$$\mathbb{E}[\mathcal{P}^m] = \left(\sum_{m=1}^{M} \mathcal{P}^m\right)/M \text{ ,and } \mathbb{E}[\mathcal{C}^m] = \left(\sum_{m=1}^{M} \mathcal{C}^m\right)/M. \tag{28}$$

C. Average Queue Length

The preamble transmission success probability provides insights on the received SINR for a random IoT device in each time slot, but does not evaluate the packets accumulation status. Many previous works have indicated that the queue length is a good indication of network congestion [3, 4]. The queue length refers to the number of packets that are waiting in buffer to be transmitted [47]. Next, we evaluate the average queue length $\mathbb{E}[Q^m]$, which denotes the average number of packets accumulated in the buffer in the mth time slot, which is derived as

$$\mathbb{E}[Q^m] = \mu_{\text{New}}^m + \mu_{\text{Cum}}^m - \mathcal{R}^m \mathcal{T}^m \mathcal{P}^m, \tag{29}$$

where μ_{Cum}^m is the intensity of number of accumulated packets in the mth time slot given in (12), μ_{New}^m is the intensity of the new arrival packets in the mth time slot, $\mathcal{P}^m$ is given in Theorem 1, $\mathcal{T}^m$ is given in Theorem 2, and $\mathcal{R}^m$ is given in Section IV.B.

VI. Numerical Results

In this section, we validate our analysis via independent system level simulations, where the BSs and IoT devices are deployed via independent PPPs in a 100 km^2 area. Each IoT device employs the channel inversion power control, and associated with its nearest BS. Importantly, the real buffer at each IoT device is simulated to capture the packets arrival and accumulation process evolved along the time. The received SINR of each active and non-deferred IoT device (i.e., IoT devices with packets and do not deferred by the ACB or the back-off mechanism) in each time slot is captured, and compared with the SINR threshold γ_{th} to determine the success or failure of each RACH attempt. Furthermore, in the ACB scheme, we also simulate that each IoT device generates a random number $q \in [0, 1]$ and compares with the ACB factor P_{ACB} to determine whether the current RACH is deferred, and in the back-off scheme, we capture all RACH failures and practically defer RACH attempts of these IoT devices for the next t_{BO} time slots. In all figures of this section, we use "Ana." and "Sim." to abbreviate "Analytical" and "Simulation", respectively. Unless otherwise stated, we set the same new packets arrival rate for each time slot ($\varepsilon_{\text{New}}^1 = \varepsilon_{\text{New}}^2 = \cdots = \varepsilon_{\text{New}}^m = 0.1$ packets/ms), $\rho = -90$ dBm, $\sigma^2 = -90$ dBm, $\lambda_B = 10$ BS/km^2, $\lambda_{Dp} = 100$ IoT deivces/preamble/km^2, $\alpha = 4$, and $\gamma_{\text{th}} = -10$ dB.

In the back-off scheme, we set that failure transmission IoT device waits 1 time slot before retransmission in the back-off scheme.

Fig. 5 plots the preamble transmission success probability $\mathcal{P}$ versus the density ratio λ_{Dp}/λ_B for various path-loss exponents (α) and various time duration ($\tau_c + \tau_g$), where the analytical plots of the preamble transmission success probability in a single time slot $\mathcal{P}$ is calculated using (7) ($\mathcal{R} = 1$). We first see the well match between the analysis and the simulation results, which validates the accuracy of developed single time slot mathematical framework. We observe that increasing the density ratio between the IoT devices and the BSs decreases the preamble transmission success probability of the 1st time slot, due to the increasing aggregate interference from more IoT devices transmitting signals simultaneously. We also notice that increasing the interval duration between RACHs decreases the preamble transmission success probability. This can be explained by the reason that the number of new arrival packets during longer interval duration increases, and leads to higher non-empty probability of IoT devices as shown in (11).
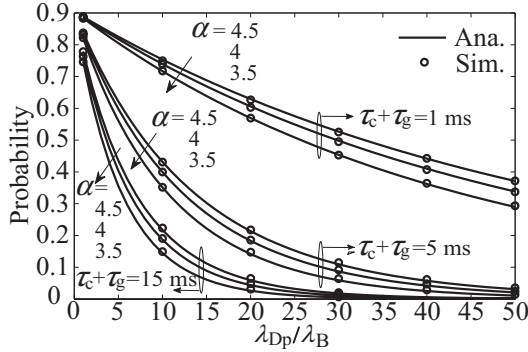

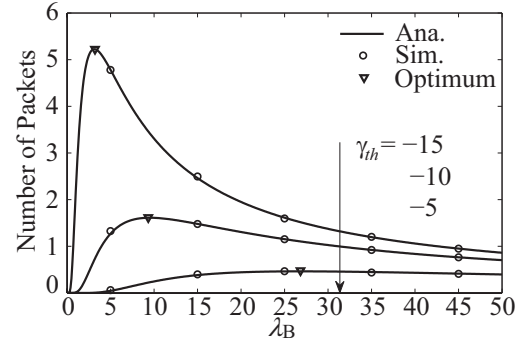Fig. 5: Preamble transmission success probability.

Fig. 6: The number of received packets per BS.

Fig. 6 plots the number of received packets per BS $\mathcal{C}$ in a single time slot versus the density of BSs λ_B for various SINR threshold γ_{th} ($\mathcal{R} = 1$). We set $\lambda_{Dp} = 500$ IoT deivces/preamble/km^2. The analytical curves for the number of received packets per BS are plotted using (26), and the optimal BSs densities that achieve the maximum number of received packets per BS are plotted using (27). We can see that the calculated optimal BS densities well predict the optimal density points achieving the maximum number of received packets per BS. The first increasing trend of the number of received packets per BS is mainly due to the improvement of the average received SINR, whereas the decreasing trend after λ_B^* is mainly due to the decreased average number of associated IoT devices of each BS leading to the reduction in channel resources utilization.

Fig. 7 plots the preamble transmission success probabilities of a random IoT device in each time slot with the baseline scheme, the ACB scheme, and the back-off scheme using (27). For

each scheme, the preamble transmission success probabilities decrease with increasing time, due to that the intensity of interfering IoT devices grows with increasing non-empty probability of each IoT device, caused by the increasing average number of accumulated packets. For each scheme, its preamble transmission success probability with $\gamma_{\mathrm{th}} = -5$ dB decreases faster than that with $\gamma_{\mathrm{th}} = -10$ dB, due to the higher chance of the accumulated packets being reduced for $\gamma_{\mathrm{th}} = -10$ dB leading to relatively lower average non-empty probability of each IoT device. Interestingly, we observe that the preamble transmission success probabilities of a random IoT device in each time slot always follow ACB($\mathrm{P}_{\mathrm{ACB}} = 0.5$)>back-off>ACB($\mathrm{P}_{\mathrm{ACB}} = 0.9$)>baseline scheme (except the 1st time slot, where the back-off procedure is not executed), this is because more strict congestion control schemes reduce more access requests from the side of IoT devices, which decrease the aggregate interference in the network.
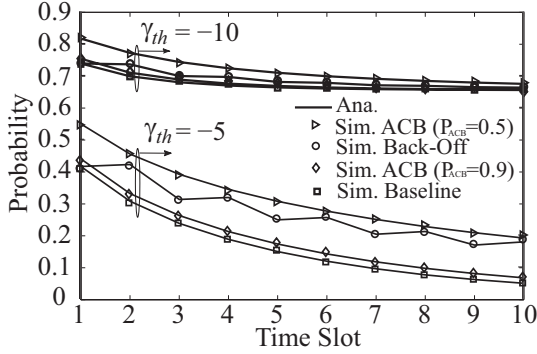

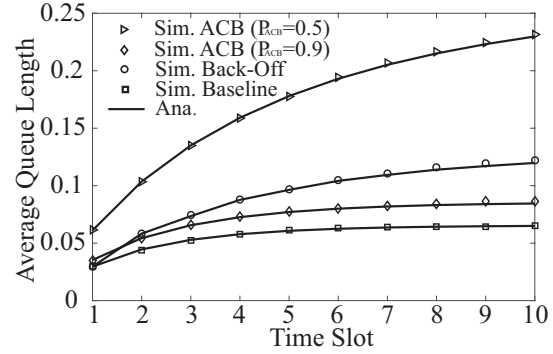Fig. 7: Preamble transmission success probability of each time slot.

Fig. 8: Average Queue Length of each time slot.

We also notice that for $\gamma_{\mathrm{th}} = -10$ dB case, the preamble transmission success probabilities with the $\mathrm{P}_{\mathrm{ACB}} = 0.5$ slightly outperform that of ACB scheme ($\mathrm{P}_{\mathrm{ACB}} = 0.9$), and the gap between them reduces with increasing time, whilst for $\gamma_{th} = -5$ dB, the preamble transmission success probabilities with $\mathrm{P}_{\mathrm{ACB}} = 0.5$ is much greater than that with $\mathrm{P}_{\mathrm{ACB}} = 0.9$, and such gap increases with increasing time. This is because for $\gamma_{\mathrm{th}} = -5$ dB, the ACB scheme $\mathrm{P}_{\mathrm{ACB}} = 0.5$ is more efficient than $\mathrm{P}_{\mathrm{ACB}} = 0.9$, in terms of providing higher average SINR by reducing the probability of queue flushing, but reversely for $\gamma_{\mathrm{th}} = -10$ dB, the ACB scheme ($\mathrm{P}_{\mathrm{ACB}} = 0.5$) has less access requests leading to lower utilization of channel resources. The preamble transmission success probability of a randomly chosen IoT device with back-off scheme is fluctuated, due to the alternation of high load and low load network condition in each time slot. Furthermore, for $\gamma_{\mathrm{th}} = -10$ dB case, the fluctuation become stable quickly, due to the accumulated packets can be handled much quicker.

In Fig 8, we plots the average queue length with $\gamma_{\mathrm{th}} = -10$ dB using (29). We observe

that the average queue length of the baseline scheme, the $\text{ACB}(\text{P}_{\text{ACB}} = 0.9)$ scheme and the back-off scheme gradually becomes steady (i.e., they become unchanging in the 10th time slot). This is due to that these schemes provides relatively faster buffer flushing that can maintain the average accumulated packets in an acceptable level. The average queue lengths follow baseline$<\text{ACB}(\text{P}_{\text{ACB}} = 0.9)$ $<$back-off$<\text{ACB}(\text{P}_{\text{ACB}} = 0.5)$ scheme, which shed lights on the buffer flushing capability of each scheme in this network condition.

(a) $\gamma_{th} = -8$ dB
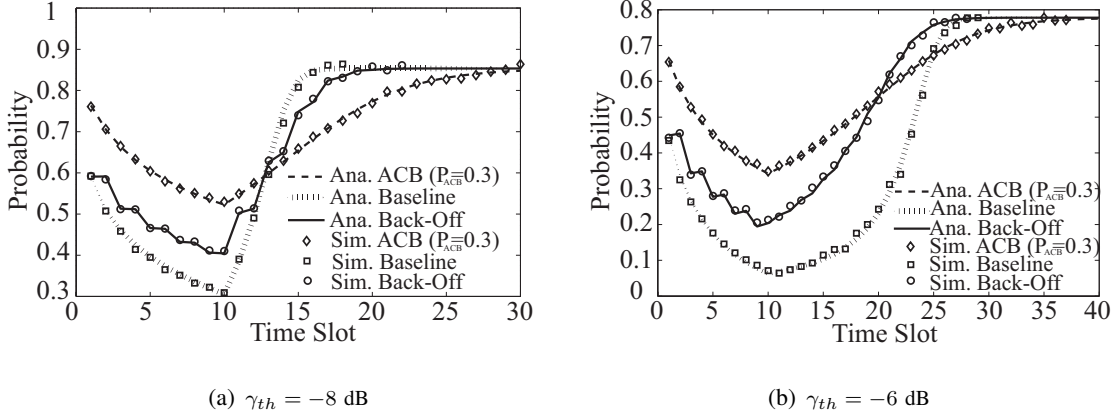
(b) $\gamma_{th} = -6$ dB

Fig. 9: Preamble transmission success probability of each time slot.

Fig. 9 plots the preamble transmission success probability of a random IoT device in each time slot with the baseline scheme, the ACB scheme, and the back-off scheme. We set $\tau_c + \tau_g = 5$ ms, ACB factor $\text{P}_{\text{ACB}} = 0.3$, and new arrival traffics only happen in the first 10 time slots ($\varepsilon_{\text{New}}^m = 0$ for $m > 10$). Note that this simulation method with new arrival traffics happen in first several time slots is to examine how well the network can handle bursty traffic, where similar practical simulations has been tested in [10, 11]. In both Fig. 9(a) and Fig. 9(b), the preamble transmission success probabilities decrease in the first 10 time slots, due to increasing traffic (new packets arrived) leading to increasing active probabilities of IoT devices. After first 10 time slots, these probabilities increase with time, due to decreasing traffic (i.e., no new packets arrive) leading to decreased active probabilities of IoT devices. After most of the accumulated packets are delivered with time, the preamble transmission success probabilities reaches the stable ceiling. Interestingly, we see that the preamble transmission success probabilities in Fig. 9(a) ($\gamma_{\text{th}} = -8$ dB) become stable earlier than that in Fig. 9(b) ($\gamma_{\text{th}} = -6$ dB), due to that the higher chance of the accumulated packets being reduced in lower threshold case.

The preamble transmission success probability of the baseline scheme increases rapidly after first 10 time slots and outperforms other two schemes after first 12th time slots in Fig. 9(a), but it increases relatively slowly after first 10 time slots and only outperforms that of the ACB

scheme after first 25 time slots in Fig. 9(b), due to that the baseline scheme provide faster buffer flushing, which leads to lower chance of the accumulated packets being reduced in relatively higher loaded network condition due to the high aggregate interference. The back-off scheme performs better than the baseline scheme in the first 10 time slots (except 1st time slot where back-off is not executed), due to that it automatically defers the retransmission requests and control the congestion in the overloaded network condition. Interestingly, it gradually outperforms the ACB scheme with strictly ACB factor $P_{\mathrm{ACB}} = 0.3$ after the first 10 time slots, due to that the back-off scheme automatically release the blocking of packets and provide faster buffer flushing than the ACB scheme in the non-overloaded network condition.

(a) The mean of preamble transmission success probabilities

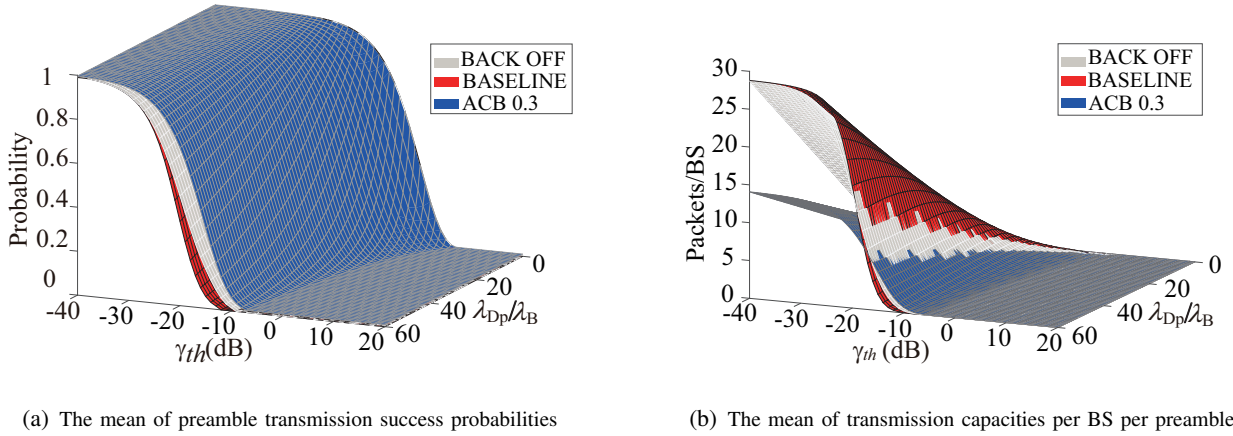(b) The mean of transmission capacities per BS per preamble

Fig. 10: The mean of preamble transmission success probabilities and the transmission capacities per BS per preamble

In Fig. 10(a) and Fig. 10(b), we plot the mean of preamble transmission success probabilities and the mean of numbers of received packets per BS over 10 time slots with each scheme, respectively. We set $\tau_g = 1$ ms and ACB factor $P_{\mathrm{ACB}} = 0.3$. Note that the new traffics arrival happen in every time slot. In Fig. 10(a), the ACB scheme always outperforms the other two schemes, and the mean of probabilities of the back-off scheme is slightly higher than that of the baseline scheme before $\gamma_{\mathrm{th}} = -25$ dB, and then such gap between the back-off scheme and the baseline scheme increase with increasing γ_{th}, which is due to that the back-off scheme blocks more packets.

In Fig. 10(b) we observe that 1) For $-40 \leq \gamma_{\mathrm{th}} \leq -25$ dB, the mean of numbers of received packets per BS with the back-off scheme is slightly lower than the baseline scheme, but nearly double that of the ACB scheme, due to the preamble transmission success probability is close to 1 as shown in Fig. 10(a), and thus less packets are blocked in the IoT device in the back-off scheme. 2) For $-25 < \gamma_{\mathrm{th}} \leq -15$ dB, the mean of numbers of received packets per BS with the baseline and the back-off schemes decrease dramatically and reduce to same level with the ACB

scheme. The back-off scheme gradually outperforms the baseline scheme around the $\gamma_{\text{th}} = -20$ and -15 dB, because the back-off scheme gradually blocks more IoT devices, and provides better network condition as well as higher probabilities of removing packets from the queue. 3) For $-15 < \gamma_{\text{th}} \leq -5$ dB, the ACB scheme outperforms the other schemes, which showcases that the ACB scheme with a relatively strict ACB factor can provide improved successful transmission in overloaded network.

VII. CONCLUSION

In this paper, we developed a spatio-temporal mathematical model to analyze the RACH of cellular-based mIoT networks. We first analyzed RACH in the single time slot, and provide the preamble detection probability performed on a randomly chosen BS, preamble transmission success probability performed on a BS associated with a randomly chosen IoT device. We then derived the preamble transmission success probabilities of a randomly chosen IoT device with baseline, ACB, and back-off schemes by modeling the queue evolution over different time slot. Our numerical results show that the ACB and back-off schemes outperform the baseline scheme in terms of the preamble transmission success probability. We also show that the baseline scheme outperforms the ACB and back-off schemes in terms of the number of received packets per BS for light traffic, and the back-off scheme performs closing to the optimal performing scheme in both light and heavy traffic conditions.

APPENDIX A

A PROOF OF LEMMA 1

The Laplace Transform of aggregate inter-cell interference can be derived as

$$
\begin{aligned}
\mathcal{L}_{I_{inter}}(s) &\stackrel{(a)}{=} E_{\widehat{\mathcal{Z}}_{out}} \Bigg[\prod_{u_i \in \widehat{\mathcal{Z}}_{out}} E_{P_i} E_{h_i} \left[e^{-sP_i h_i \|u_i\|^{-\alpha}} \right] \Bigg] \\
&\stackrel{(b)}{=} \exp\left(-2\pi \mathcal{T}^m \mathcal{R}^m \lambda_{Dp} \int_{(P/\rho)^{\frac{1}{\alpha}}}^{\infty} E_P E_h \left[1 - e^{-sPhx^{-\alpha}} \right] x dx \right) \\
&\stackrel{(c)}{=} \exp\left(-2\pi \mathcal{T}^m \mathcal{R}^m \lambda_{Dp} \int_{(P/\rho)^{\frac{1}{\alpha}}}^{\infty} E_P \left[1 - \frac{1}{1 + sPx^{-\alpha}} \right] x dx \right) \\
&\stackrel{(d)}{=} \exp\left(-2\pi \mathcal{T}^m \mathcal{R}^m \lambda_{Dp} s^{\frac{2}{\alpha}} E_P[P^{\frac{2}{\alpha}}] \int_{(s\rho)^{\frac{-1}{\alpha}}}^{\infty} \frac{y}{1 + y^\alpha} dy \right),
\end{aligned}
\tag{A.1}
$$

where $s = \gamma_{\text{th}}/\rho$, $E_x[*]$ is the expectation with respect to the random variable x, (a) follows from independence between λ_{Dp}, P_i, and h_i, (b) follows from the probability generation functional

(PGFL) of the PPP, (c) follows from the Laplace Transform of h, and (d) obtained by changing the variables $y = \frac{x}{(SP)^{\frac{1}{\eta}}}$. The kth moments of the transmit power is expressed as [30]

$$E_P[P^k] = \frac{\rho^k \gamma(\frac{k\alpha}{2} + 1, \pi\lambda_B(\frac{P}{\rho})^{\frac{2}{\alpha}})}{(\pi\lambda_B)^{\frac{k\alpha}{2}}(1 - e^{-\pi\lambda_B(\frac{P}{\rho})^{\frac{2}{\alpha}}})}, \quad (A.2)$$

where $\gamma(a, b) = \int_0^b t^{a-1}e^{-t}dt$ is the lower incomplete gamma function. As mentioned earlier, the transmit power of IoT device is large enough for uplink path-loss inversion, while not violating its own maximum transmit power constraint, and thus The moments of the transmit power is obtained as

$$E_P[P^{\frac{2}{\alpha}}] = \frac{\rho^{\frac{2}{\alpha}}}{\pi\lambda_B}. \quad (A.3)$$

Substituting (A.3) into (A.1), we derive the Laplace Transform of aggregate inter-cell interference.

APPENDIX B

A PROOF OF LEMMA 2

The Laplace Transform of aggregate intra-cell interference is conditioned on known the number of interfering intra-cell IoT devices Z_B given as

$$\mathcal{L}_{\mathcal{I}_{intra}}(s) = \sum_{n=0}^{\infty} \mathbb{P}\{Z_B = n\}\left(E\left[e^{-sI}\right]\big| Z_B = n\right)$$

$$= \mathbb{P}\{Z_B = 0\} + \sum_{n=1}^{\infty} \mathbb{P}\{Z_B = n\}\left(E_{h_n}\left[\exp\left(-s\sum_{1}^{n}\rho h_n\right)\right]\right)$$

$$\overset{(a)}{=} \mathbb{P}\{Z_B = 0\} + \sum_{n=1}^{\infty} \mathbb{P}\{Z_B = n\}\left(\frac{1}{1 + s\rho}\right)^n, \quad (B.1)$$

where $s = \gamma_{\text{th}}/\rho$, $\mathbb{P}\{Z_B = n\}$ is the probability of the number of interfering intra-cell IoT devices $Z_B = n$ given in (9), and (a) follows from the Laplace Transform of h_n. After some mathematical manipulations, we proved (6) in Lemma 2.

REFERENCES

[1] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of things for smart cities," *IEEE Internet Things J.*, vol. 1, no. 1, pp. 22–32, Feb. 2014.

[2] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (IoT): A vision, architectural elements, and future directions," *Future Gener. Comp. Sy.*, vol. 29, no. 7, pp. 1645–1660, Sep. 2013.

[3] M. Hasan, E. Hossain, and D. Niyato, "Random access for machine-to-machine communication in LTE-advanced networks: issues and approaches," *IEEE Commun. Mag.*, vol. 51, no. 6, pp. 86–93, Jun. 2013.

[4] A. Laya, L. Alonso, and J. Alonso-Zarate, "Is the random access channel of LTE and LTE-A suitable for M2M communications? A survey of alternatives." *IEEE Commun. Surveys Tuts.*, vol. 16, no. 1, pp. 4–16, Jan. 2014.

[5] "Study on RAN improvements for machine-type communications," *3GPP, Sophia, Antipolis, France, TR 37.868 V11.0.0,*, Sep. 2011.

[6] A. G. Gotsis, A. S. Lioumpas, and A. Alexiou, "M2M scheduling over LTE: Challenges and new perspectives," *IEEE Veh. Technol. Mag.*, vol. 7, no. 3, pp. 34–39, Sept. 2012.

[7] A. Ksentini, Y. Hadjadj-Aoul, and T. Taleb, "Cellular-based machine-to-machine: overload control," *IEEE Netw.*, vol. 26, no. 6, pp. 54–60, Nov. 2012.

[8] Nokia, "LTE evolution for IoT connectivity," *White Paper*, 2016. [Online]. Available: http://resources.alcatel-lucent.com/asset/200178

[9] Ericsson, "Cellular networks for massive IoT - enabling low power wide area applications," *White Paper*, 2016. [Online]. Available: https://www.ericsson.com/res/docs/whitepapers/wp_iot.pdf

[10] "[70bis11] – LTE: MTC LTE simulations," *3GPP, ZTE, Madrid, Spain, 3GPP TSG RAN WG2 71 R2-104663*, Aug. 2010.

[11] "Evaluation of RACH congestion solutions," *3GPP, ZTE, Stockholm, Sweden, TSG RAN WG2 R2 103742*, Jun. 2010.

[12] A. Biral, M. Centenaro, A. Zanella, L. Vangelista, and M. Zorzi, "The challenges of M2M massive access in wireless cellular networks," *Digital Commun. and Netw.*, vol. 1, no. 1, pp. 1–19, Feb. 2015.

[13] E. Dahlman, S. Parkvall, and J. Skold, *4G: LTE/LTE-advanced for mobile broadband*. Academic press, 2013.

[14] Z. Alavikia and A. Ghasemi, "A multiple power level random access method for M2M communications in LTE-A network," *Trans. on Emerg. telecommun. technol.*, 2016.

[15] A. G. Gotsis, A. S. Lioumpas, and A. Alexiou, "Evolution of packet scheduling for machine-type communications over LTE: algorithmic design and performance analysis," in *IEEE Global Commun. Conf. (GLOBECOM)*. IEEE, Dec. 2012, pp. 1620–1625.

[16] I. Leyva-Mayorga, L. Tello-Oquendo, V. Pla, J. Martinez-Bauset, and V. Casares-Giner, "Performance analysis of access class barring for handling massive M2M traffic in LTE-A networks," in *Int. Conf. Commun. (ICC)*. IEEE, 2016, pp. 1–6.

[17] G.-Y. Lin, S.-R. Chang, and H.-Y. Wei, "Estimation and adaptation for bursty LTE random access," *IEEE Trans. Veh. Technol.*, vol. 65, no. 4, pp. 2560–2577, Apr. 2016.

[18] K. Zheng, F. Hu, W. Wang, W. Xiang, and M. Dohler, "Radio resource allocation in LTE-advanced cellular networks with M2M communications," *IEEE Commun. Mag.*, vol. 50, no. 7, Jul. 2012.

[19] S. Dama, T. V. Pasca, V. Sathya, and K. Kuchi, "A novel RACH mechanism for dense cellular-IoT deployments," in *Wireless Commun. Netw. Conf. (WCNC), 2016 IEEE*. IEEE, Apr. 2016, pp. 1–6.

[20] P. Wali, D. Das *et al.*, "Optimal time-spatial randomization techniques for energy efficient IoT access in LTE-Advanced," *IEEE Trans. Veh. Technol.*, Feb. 2017.

[21] P. Zhou, H. Hu, H. Wang, and H.-h. Chen, "An efficient random access scheme for OFDMA systems with implicit message transmission," *IEEE Trans. wireless Commun.*, vol. 7, no. 7, Jun. 2008.

[22] C.-H. Wei, G. Bianchi, and R.-G. Cheng, "Modeling and analysis of random access channels with bursty arrivals in OFDMA wireless networks," *IEEE Trans. Wireless Commun.*, vol. 14, no. 4, pp. 1940–1953, Apr. 2015.

[23] T. D. Novlan, H. S. Dhillon, and J. G. Andrews, "Analytical modeling of uplink cellular networks," *IEEE Trans. Wireless Commun.*, vol. 12, no. 6, pp. 2669–2679, Jun. 2013.

[24] J. G. Andrews, F. Baccelli, and R. K. Ganti, "A tractable approach to coverage and rate in cellular networks," *IEEE Trans. Commun.*, vol. 59, no. 11, pp. 3122–3134, Nov. 2011.

[25] S. M. Yu and S. L. Kim, "Downlink capacity and base station density in cellular networks," in *Proc. Int. Symp. Modeling Mobile Ad Hoc WiOpt Netw.*, May. 2013, pp. 119–124.

[26] Y. Deng, L. Wang, M. Elkashlan, A. Nallanathan, and R. K. Mallik, "Physical layer security in three-tier wireless sensor networks: A stochastic geometry approach," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 6, pp. 1128–1138, Jun. 2016.

[27] Y. Deng, L. Wang, S. A. R. Zaidi, J. Yuan, and M. Elkashlan, "Artificial-noise aided secure transmission in large scale spectrum sharing networks," *IEEE Trans. Commun.*, vol. 64, no. 5, pp. 2116–2129, May. 2016.

[28] H. ElSawy, E. Hossain, and M. Haenggi, "Stochastic geometry for modeling, analysis, and design of multi-tier and cognitive cellular wireless networks: A survey," *Commun. Surveys Tuts.*, vol. 15, no. 3, pp. 996–1019, Jul. 2013.

[29] Y. Deng, L. Wang, M. Elkashlan, M. Di Renzo, and J. Yuan, "Modeling and analysis of wireless power transfer in heterogeneous cellular networks," *IEEE Trans. Commun.*, vol. 64, no. 12, pp. 5290–5303, Dec. 2016.

[30] H. ElSawy and E. Hossain, "On stochastic geometry modeling of cellular uplink transmission with truncated channel inversion power control," *IEEE Trans. Wireless Commun.*, vol. 13, no. 8, pp. 4454–4469, Aug. 2014.

[31] Y. Zhong, T. Q. Quek, and X. Ge, "Heterogeneous cellular networks with spatio-temporal traffic: Delay analysis and scheduling," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 6, pp. 1373–1386, 2017.

[32] K. Stamatiou and M. Haenggi, "Random-access Poisson networks: stability and delay," *IEEE Commun. Lett.*, vol. 14, no. 11, pp. 1035–1037, Nov. 2010.

[33] Y. Zhong, M. Haenggi, T. Q. Quek, and W. Zhang, "On the stability of static Poisson networks under random access," *IEEE Trans. Commun.*, vol. 64, no. 7, pp. 2985–2998, Jul. 2016.

[34] M. Gharbieh, H. ElSawy, A. Bader, and M.-S. Alouini, "Spatiotemporal stochastic modeling of IoT enabled cellular networks: Scalability and stability analysis," *IEEE Trans. Commun.*, May. 2017.

[35] L. Chen, W. Chen, X. Zhang, and D. Yang, "Analysis and simulation for spectrum aggregation in LTE-advanced system," in *70th Veh. Technol. Conf. (VTC Fall).* IEEE, 2009, pp. 1–6.

[36] K. Zhou, N. Nikaein, and T. Spyropoulos, "LTE/LTE-A discontinuous reception modeling for machine type communications," *IEEE Commun. Lett.*, vol. 2, no. 1, pp. 102–105, Feb. 2013.

[37] S. N. Chiu, D. Stoyan, W. S. Kendall, and J. Mecke, *Stochastic geometry and its applications.* John Wiley & Sons, 2013.

[38] A. Goldsmith, *Wireless communications.* Cambridge university press, 2005.

[39] "Evolved universal terrestrial radio access (E-UTRA): physical channels and modulation," *3GPP, TS 36.211 v.13.2.0, Release 13*, 2016.

[40] T. Kim, I. Bang, and D. K. Sung, "An enhanced PRACH preamble detector for cellular IoT communications," *IEEE Commun. Lett.*, vol. 21, no. 12, pp. 2678–2681, Dec. 2017.

[41] H. M. Gursu, M. Vilgelm, W. Kellerer, and M. Reisslein, "Hybrid collision avoidance-tree resolution for M2M random access," *IEEE Trans. Aerosp. Electron. Syst.*, Mar. 2017.

[42] M. N. Soorki, W. Saad, M. H. Manshaei, and H. Saidi, "Stochastic coalitional games for cooperative random access in M2M communications," *IEEE Trans. Wireless Commun.*, Jun. 2017.

[43] G. Gow and R. Smith, *Mobile and wireless communications: an introduction.* McGraw-Hill Education (UK), 2006.

[44] M. Haenggi, *Stochastic geometry for wireless networks.* Cambridge University Press, 2012.

[45] B. Francois and B. Bartlomej, "Stochastic geometry and wireless networks," *B. NoW Publishers: Paris*, pp. 10–10, 2009.

[46] J.-S. Ferenc and Z. Néda, "On the size distribution of Poisson Voronoi cells," *Phys. A: Statistical mech. appl.*, vol. 385, no. 2, pp. 518–526, Nov. 2007.

[47] A. S. Alfa, *Queueing theory for telecommunications: discrete time modelling of a single node system.* Springer Science & Business Media, 2010.