IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received May 24, 2017, accepted June 15, 2017, date of publication June 21, 2017, date of current version July 17, 2017.

Digital Object Identifier 10.1109/ACCESS.2017.2717818

Packet-Based Preamble Design for Random Access in Massive IoT Communication Systems

JUN ZOU[1], HAI YU[1], WEIWEI MIAO[2], AND CHENGLING JIANG[2]
[1]Wireless Network and Mobile Communication Group, Nanjing University of Science and Technology, Nanjing 210094, China
[2]Information and Telecommunication Branch, State Grid Jiangsu Electric Power Company, Nanjing 210024, China

Corresponding author: Jun Zou (jun_zou@njust.edu.cn)

This work was supported in part by the Fundamental Research Funds for the Central Universities under Grant 30917011318 and in part by the technology project of the State Grid Jiangsu Electric Power Company.

ABSTRACT The Internet of Things (IoT), which is a network that enables devices in the network to exchange information, has rapidly developed in recent years. Wireless communication technologies on the IoT are the best way to solve the ''last mile'' problem and gain substantial attention. The low power consumption and low cost are notably important for the IoT devices that are called massive IoT (mIoT). Narrow-band communication is one of the solutions to reduce the cost and power consumption and is considered the solution to large coverage without an available spectrum. Large coverage also implies a long transmission time interval, which makes the random access process in the current LTE system unsuitable for mIoT applications. The random access process in the current LTE system is notably complex with some handshakes to exchange information between the base station and the device. We address the issue in this paper and propose a packet-based preamble to simplify the random access process to decrease battery consumption.

INDEX TERMS Random access, preamble detection, timing.

I. INTRODUCTION

The Internet of Things (IoT) aims to connect all objects in the world and enable them to exchange information [1], [2]. With the rapid development of wireless communication technologies, the IoT is step by step realized in recent years. The development of the IoT industry also promotes the evolution of wireless communication technologies, which is the key to solving the ''last mile'' problem. The IoT has been the main scenario of recent wireless communication and poses some challenges. In general, there are two types of IoT applications. One is the massive IoT (mIoT), whose characteristics are mass access devices, latency tolerance and low cost, with applications in power utilization collection, meter auto reporting, smart parking and so on [3]–[5]. The other is mission-critical IoT with the strict requirement of low latency, such as self-driving car, e-health, and industry automation [2], [6]. According to the research of Cisco, there will be more than 25 billion IoT devices, of which 60% are mIoT applications.

Because there are many devices and most mIoT devices use batteries, low cost and low power consumption are the most important requirements. The time during which the device transmits and receives signals determines the battery consumption. Random access is the process for the device to register or send a schedule request to the network. For the current LTE system (including the LTE-eMTC [7]), the random access process is accomplished using a random access preamble and some handshakes between the base station and the device, which is optimized for human-type communication (HTC). However, it is not suitable for the mIoT. For the mIoT, the maximum coupling loss is at least 15 dB more than the HTC, which implies that more transmission time is required by each information exchange between the device and the base station [3]. The complex random access process is not optimized to the battery consumption. Thus, this paper focuses on the design of a simplified random access for mIoT to satisfy the lower battery consumption in the bands that are narrower than 1.08 MHz, particularly the 200-kHz bands, where a legacy LTE (including LTE-eMTC) system fails to work.

In Section II, we briefly review the LTE random access scheme. Section III provides a battery consumption analysis and proposes a packet-based preamble design. Section IV provides the simulation results to verify the proposed design. Finally, Section V concludes this paper.

II. LTE RANDOM ACCESS

A device wakes up in response to the event of data arrival, e.g., as a result of reporting a meter reading from the device's upper application layer. Because of the random nature of this

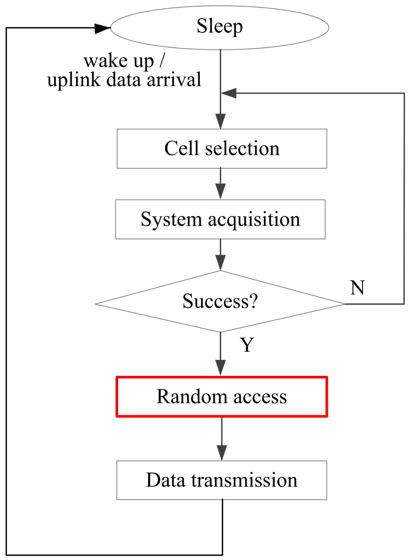

FIGURE 1. **Procedures involved in a typical wakeup of a device for application data transmission in a cellular system.**

type of event, a random access mechanism must be used to gain access to the cellular network. In this section, we briefly review the LTE random access scheme.

Fig. 1 shows typical operations that a device performs in response to an uplink data transfer request. After waking up, the device obtains a cell ID from the cell selection protocol, which is usually the ID of the most recently used cell. The device performs a system acquisition by searching for the downlink synchronization signals of the cell. If found, the device synchronizes its local timing and frequency to the synchronization signals, which include a one-way propagation delay in timing. As soon as the timing and frequency are acquired, the device locates the downlink broadcast channel and decodes the system information, e.g., the uplink random access resource configuration. If the synchronization signals of the cell are not found, the device goes back to the cell selection procedure and looks for the next candidate cell listed in the preferred roaming list (PRL), which is provided by the operator.

Since in sleep, all resources (through which the device communicates with the network access point or the base station) are released back to the network, the device needs to request resources from the network upon waking up from the sleep in order to re-establish a communication link with the network. This task is accomplished using a random access mechanism.

Fig.2 (a) shows the LTE random access signal flow, which is initiated by a preamble transmitted by the device on the resources (specified in the system information) that are specifically reserved for the random access purpose.

An LTE random access preamble is a Zadoff-Chu (ZC) sequence-based CDMA (code division multiple access) signal that is time-frequency spread over the entire uplink random access resources (referred to as the Physical Random Access Channel or PRACH in LTE terminology) and occupy 1.08 MHz of the total system bandwidth shared among all devices [8]–[10]. Before the preamble can be transmitted, a device estimates the path loss via the downlink signals. Then, the device randomly selects a preamble from a pool of 64 waveforms and transmits it on PRACH at the exactly sufficient power to compensate for the path loss to minimize the near-far effect. Since the transmission timing is obtained from the downlink synchronization signals, the arrival time at the network access point or base station contains a round-trip (i.e., downlink plus uplink) propagation delay. The base station constantly detects the presence of any of the 64 preambles on the random access resources within a search window that is sufficiently large to accommodate the largest round-trip delay (determined by the cell size). If detected, the "random access response message" is transmitted on the downlink traffic channel (or PDSCH in LTE terminology). The random access response message contains the detected preamble index and its associated information, including the 11-bit time advance command, the 16-bit temporary identifier for further communications between this device and the base station, and the uplink data channel (PUSCH) resource configuration (20 bits) for the device to transmit the subsequent contention resolution message. Note that the temporary identifier is not valid until the device wins the contention. The time advance is equal to the round-trip propagation delay of the detected device, Δt (estimated from the preamble), for use by the device to advance its transmission time (by Δt) to compensate for the round-trip propagation delay. Then, the signals from different devices become time-aligned at the base station receiver such that a smaller CP can be used on the uplink traffic channel (i.e., PUSCH) to absorb just the multipath spread.

On the device side, once the preamble is sent, it monitors the corresponding random access response messages on PDSCH. A failure to receive the response from the base station can be the results of insufficient transmit power and/or a miss of detection by the base station. The device then restarts the same procedure with increased preamble power. If the decoded message contains the preamble index that the device has used, the device advances its timing (indicated in this message) and transmits the contention resolution message on the specified PUSCH resources (the first scheduled transmission on uplink). The contention resolution is necessary since more than one device may have used the same preamble waveform (i.e., a collision), and the device has not yet had confirmation that the response is intended for it rather than another device.

The contention resolution message contains a 40-bit "contention resolution key" (e.g., the device's unique identification within the network). If the base station successfully decodes the message, a contention resolution response that mirrors the received contention resolution message is transmitted and addressed to the device with the same contention resolution key. A failure to receive the message from the base station can be the result of collision, and the device has to restart the procedure from the beginning.

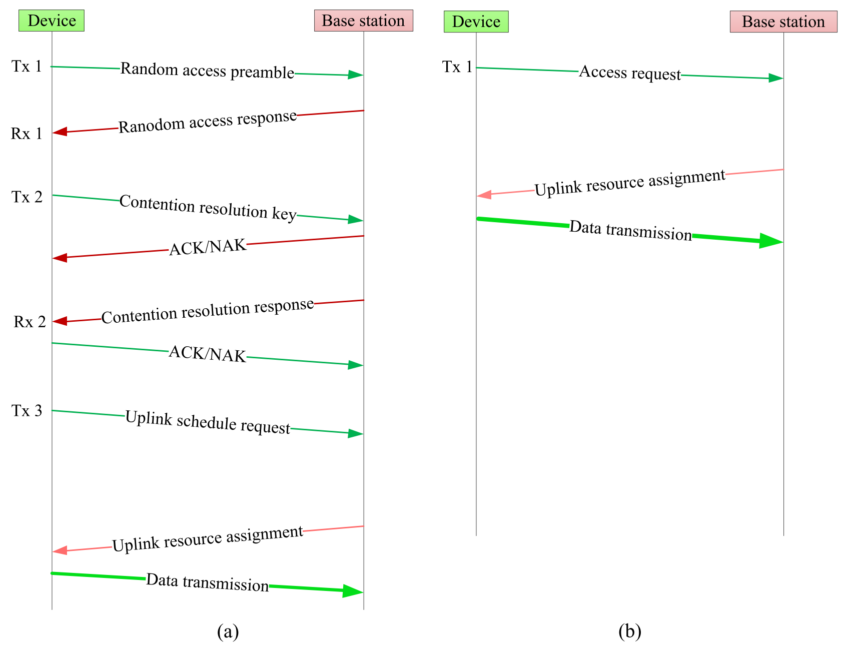

FIGURE 2. Illustration of random access signaling and uplink data transmission in (a) Legacy LTE, and (b) simplified random access for the mIoT.

We see that the LTE random access involves a sequence of message exchanges between a device and the base station. This presents excessive overhead that is not optimized for mIoT but for HTC. In the next section, we propose a packet-based preamble design to simplify the random access process.

III. PACKET-BASED RANDOM ACCESS DESIGN

A. BATTERY CONSUMPTION ANALYSIS

A device's battery life is crucial to most mIoT applications and hence the main focus of the design and optimization.

Depending on the type of mIoT device, the typical capacity of the battery ranges from 500 mAh (e.g., for a smart watch) to 5000 mAh (e.g., for a metering device). The required battery life for mIoT ranges from days to years.

During reception, the current drawn from a battery is roughly by baseband processing I_0, i.e.,

$$I_{\mathrm{Rx}} \approx I_0, \tag{1}$$

whereas during transmission, the total current is drawn by the signal transmission plus baseband processing. It can be approximated as

$$I_{\mathrm{Tx}} \approx I_0 + \frac{p/\eta}{V}, \tag{2}$$

where p is the transmit power, V is the battery voltage (e.g., 3 V), and η is the power amplifier efficiency ranging from 10% to 40%. A typical value of I_0 is on the order of 150 mA. Assuming that the maximum transmit power of the device is 20 dBm, $I_0 = 150$ mA, and $\eta = 30\%$, the total current drawn is 150 mA during reception and 260 mA during transmission, which is much greater than the current pulled from the battery when the device is in deep sleep (on the order of a few micro-Amps).

Thus, the battery consumption per random access is

$$C = t_{\mathrm{Tx}} I_{\mathrm{Tx}} + t_{\mathrm{Rx}} I_{\mathrm{Rx}}, \tag{3}$$

where t_{Tx} and t_{Rx} are the total transmission and receiving time during a random access process, respectively. The actual values of t_{Tx} and t_{Rx} depend on the random access design. Nevertheless, it is clear that the device's "air time", particularly the transmit time, has a profound effect on the battery life, and its optimization is vital to most mIoT applications.

B. TRANSMISSION BANDWIDTH ANALYSIS

According to Shannon capacity theory, the capacity has a positive relationship with the transmission bandwidth. However, for a fixed bandwidth resource, a larger bandwidth used by a device corresponds to a smaller access device number. Obviously, there is a tradeoff between the system capacity and the transmission delay of each device. In this section, we analyze the suboptimal transmission bandwidth for the mIoT devices in the uplink transmission.

The receive SNR (operating SNR) Γ is calculated as

$$\Gamma(w) = p - \Delta - (N_0 + \eta + w) \ \ \mathrm{dB} \tag{4}$$

where p (dBm) is the device transmit power, Δ(dB) is the maximum coupling loss (pathloss) in the mIoT scenario, N_0 (dBm/Hz) is the noise power spectral density, η (dB) is the noise figure of the receiver at the base station, and w (dB $\cdot$ Hz) is the transmission bandwidth. Then, the transmission time of a message with size $|\mathscr{M}|$ can be expressed as

$$\tau\,(w) = |\mathscr{M}|/w \log_2(1 + \beta \cdot 10^{\frac{\Gamma(w)}{10}}) \tag{5}$$

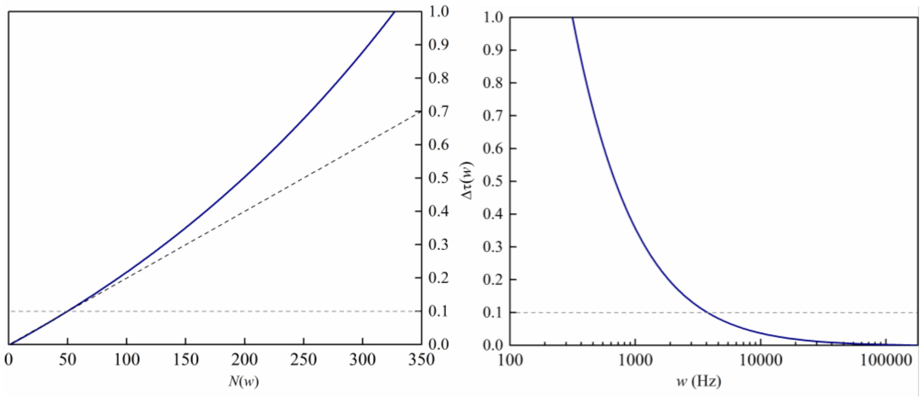

FIGURE 3. **(a) plot of the relationship between the system capacity and the time punishment defined in (6); (b) plot of the relationship between the transmission bandwidth and the time punishment, where $p = 20$ dBm, $\Delta = 155$ dB, $N_0 = -174$ dBm/Hz, $\eta = 3$ dB, $W = 180$ KHz, $\beta = -5$ dB, and $|\mathscr{M}| = 1000$ bits.**

where β is used to compensate the performance difference between a realistic system and the Shannon capacity limit. When the system bandwidth is W, the percentage of increased transmit time (time punishment) with bandwidth w compared to using the system bandwidth can be defined as

$$\Delta\tau(w) = \frac{\tau(w) - \tau(W)}{\tau(W)} = \frac{W \log_2(1 + \cdot 10^{\frac{\Gamma(W)+\beta}{10}})}{w \log_2(1 + 10^{\frac{\Gamma(w)+\beta}{10}})} - 1. \quad (6)$$

The maximum number of users who transmit on bandwidth w in one second, which is also called the system capacity, can be written as

$$N(w) = \frac{W/w}{\tau(w)}. \quad (7)$$

Fig. 3 shows the relationship among the transmit time punishment, transmission bandwidth and system capacity. Thus, a larger transmission bandwidth w corresponds to less time punishment $\Delta\tau(w)$, which also implies a lower battery consumption. However, the effect of increasing the transmission bandwidth on the reduction of transmission time diminishes with the increase in transmission bandwidth. In other words, there is a suboptimal transmission bandwidth w_0. For $w > w_0$, the device becomes more power-limited instead of bandwidth-limited, i.e., allocating more bandwidth provides limited help in reducing the transmission time.

If we define the suboptimal transmission bandwidth as w_0, at which $\Delta\tau(w_0)$ equals, e.g., 10%, the w_0 will be is approximately 4 KHz. In addition, the change slope between $N(w)$ and $\Delta\tau(w)$ is nearly linear at approximately the transmission bandwidth w_0 and becomes steeper when the time punishment increases. In other words, the capacity increment diminishes with the increase in time punishment. Thus, w_0 of approximately 4 KHz is the suboptimal transmission bandwidth for the consideration of transmission time (battery consumption) and system capacity. Additionally, considering the interference constraint between mIoT and the legacy LTE system, 3.75 KHz is a better choice for the suboptimal transmission bandwidth, which can be an exact division of 15 KHz (legacy LTE subcarrier spacing). The suboptimal transmission bandwidth is identical to that of the NB-IoT [8].

C. SIMPLIFIED RANDOM ACCESS SIGNALING

The primary purpose of the preamble in the legacy mobile broadband LTE random access is 1) to indicate to the base station the presence of an accessing device, and 2) to provide the base station a means of measuring the uplink timing offset (i.e., the round-trip propagation delay) of the device. The handshakes that follow the preamble are for the base station to provide the access device with a unique and shortened identifier within the cell for the subsequent data communications between the base station and the device. These two goals are accomplished by a single special OFDM signal in the following design.

As illustrated in Fig. 4, each random access channel occupies one subcarrier out of a total of $S = 48$ subcarriers, thereby constituting a total of $N_{\text{RACH}} = 48$ random access channels, each of which has a bandwidth of $w = W/N_{\text{RACH}} = 3.75$KHz according to the bandwidth analysis in the last section, where $W = 180$KHz is the total bandwidth. The random access signal, which is transmitted on one of the random access channels by a device, consists of N_{OFDM} special OFDM symbols. Each OFDM symbol is equipped with an extended CP (longer than the traffic channel CP, e.g., $T_{\text{CP}} = 35\ \mu$s for a cell size of 5 km, which is only used for the multipath delay spread) to absorb the multipath spread and round-trip propagation delay to enable the decoding of the access request message $\mathscr{M}$ carried by the packet-based preamble from a device without the knowledge of the arrival timing of each individual random access signal (since uplink timing has not yet been established at this point). Note that the use of a longer CP increases the overhead of an OFDM symbol. Nevertheless, this effect can be compensated by using a longer OFDM symbol (i.e., smaller subcarrier spacing) compared to the legacy LTE system.

The message $\mathscr{M}$ contains a 10-bit access ID, 4-bit resource request, and 10-bit CRC, resulting in a message that has

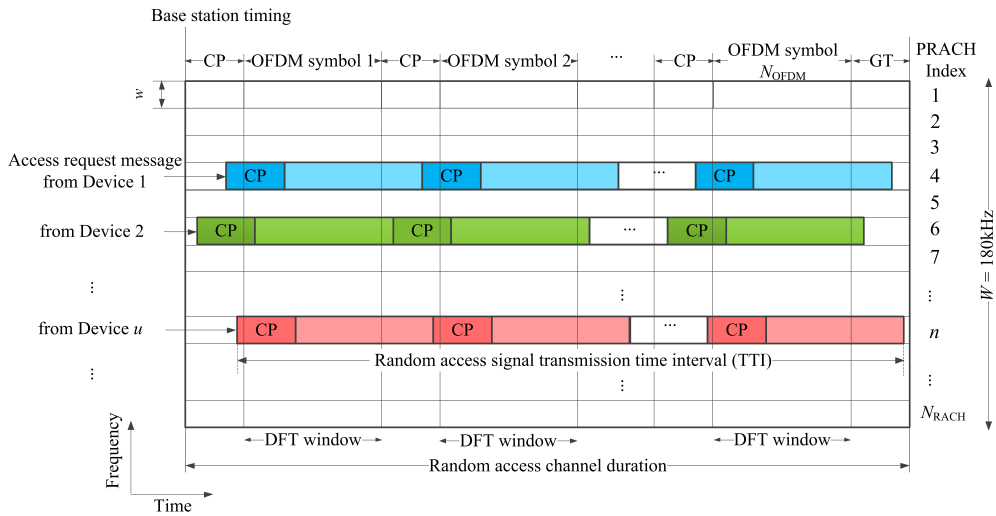

FIGURE 4. **Illustration of the random access signal structure and the physical random access channel timing at the base station receiver, where the guard time, denoted as GT, prevents random access signals from leaking into the following transmission region (where traffic channels reside). The N_{OFDM} OFDM symbols constitute N_{RACH} frequency division multiplexed (FDM) random access channels for devices to signal scheduling requests to the base station. In this example, device 1 selects channel 4, device 2 selects channel 6, and device *u* selects channel *n*. The base station uses an extended CP (longer than the traffic channel CP) to absorb not only the multipath delay spread but also the *various-length* propagation delays from devices. The DFT windows (fixed) are used by the base station to extract the OFDM symbols that contain the *N* access request messages from the *N* devices.**

$|\mathscr{M}| = 24$ information bits. This message is channel-coded (tail-biting-convolutional coding), QPSK modulated, and cell-specifically scrambled to produce a sequence of modulation symbols, which are further mapped onto the resource elements of the random access channel that is randomly selected by the device from a pool of N_{RACH} channels (cf. Fig. 4). The access ID is also randomly selected by the device from a pool of 2^{10} IDs. Like the temporary identifier in LTE, the access ID is used for the identification of a device in the current access within the current cell. Here the 4-bit uplink resource request is used to indicate the volume of the uplink data for the uplink resource allocation.

As shown in Fig. 4, using the base station timing, the base station extracts N_{OFDM} OFDM symbols without the need for the knowledge of the arrival time of each individual device, $\Delta t_u > 0$, and $u \in \{1, 2, \cdots, U\}$ (where U is the number of access devices in the current random access occasion) due to the use of the extended CP, and then tries to decode the N_{RACH} potential messages on the N_{RACH} random access channels. For notational simplification, we drop the device index, u, without causing confusion.

In the current scheme, the presence of an access device is detected by a successful decoding of an access request message as indicated by a CRC check whereas in legacy LTE (or eMTC) it relies on the detection of the preamble waveform based on a threshold which is a function of the number of preamble waveforms (64 ZC sequences in LTE) and the level of instantaneous interference from other accessing devices (which is hard to be accurately estimated). The detection is inefficient due to the use of an overly-high threshold in order to keep the rate of false detection manageable, and due to the fact that the larger the pool of waveforms is, the less the detection efficiency. A low detection probability of the preamble means more preamble transmissions for an access device, and hence more power consumptions. In this sense, the proposed scheme has a clear advantage owing to the more reliable CRC check. In the current scheme, the access preamble detection false alarm rate is determined by the CRC error probability, which is $\sim 2^{-10} \approx 0.001$ for a 10-bit CRC. A 12-bit CRC then gives a false alarm rate of $2^{-12} \approx 0.00024$.

When a device's access request message $\mathscr{M}$ is detected on one of the N_{RACH} random access channels as a result of a successful decoding of $\mathscr{M}$ (i.e., CRC checks), an uplink resource assignment for uplink data uploading is sent through the downlink control channel (i.e., EPDCCH [11]) addressed to the device with the access ID indicated in $\mathscr{M}$ for data transmission. Fig.2 (b) draws the simplified call flow, for comparison with the legacy LTE in Fig.2 (a).

A collision happens whenever more than one device happen to select the same random access channel with a probability of

$$p_{ch} = 1 - \left(\frac{N_{RACH} - 1}{N_{RACH}}\right)^{U-1} = 1 - \left(1 - \frac{1}{N_{RACH}}\right)^{U-1}, \tag{8}$$

where U is the number of concurrent accessing devices.

In the legacy LTE random access, the temporary device identifier is assigned by the base station, while in the current proposed design, it is randomly chosen by the device itself. A collision happens when more than one device choose the same access ID. The corresponding probability is

$$p_{\rm ID} = 1 - \left(1 - \frac{1}{N_{\rm ID}}\right)^{U-1}, \tag{9}$$

where $N_{\rm ID} = 2^{10}$ is the number of available IDs for selection. The total collision probability is then

$$p_{\rm c} = 1 - (1 - p_{\rm ch})(1 - p_{\rm ID}). \tag{10}$$

Since the number of available access IDs ($N_{\rm ID}$) is, by design, much greater than the number of random access channels ($N_{\rm RACH}$), $p_{\rm ch} \gg p_{\rm ID}$. Therefore, $p_{\rm c} \approx p_{\rm ch}$. That is, the collision is dominated by the access channel collision whose probability is in reverse proportion to the number of random access channels. The consequence of the channel collision is most likely a failure to decode the message by the base station. The device then will not receive the resource assignment from the base station. Another round of random access attempt at the next random access opportunity is necessary, thereby resulting in increased total transmission time. When U is 5, $p_{\rm c} \approx p_{\rm ch} \approx 0.09$ is acceptable.

D. TIMING ESTIMATION

As noted in above, a preamble is used mainly to indicate the presence of an access device and provide a means to measure the uplink timing (round-trip propagation delay) at the base station. Based on the arrival time measurement from the preamble, the base station instructs the device to advance its uplink timing to compensate for the round-trip propagation delay, so that the uplink signals from different devices are time-aligned at the base station. Then, a smaller CP can be used to absorb the multi-path delay and timing errors for subsequent uplink transmissions on the traffic channels. In the current simplified random access design, the presence of an access device is indicated by the successful decoding of its access request message, and the necessity for the knowledge of propagation delay is negated by using a larger CP (e.g., 35μs). However, the time of arrival estimation for each access device remains necessary for subsequent uplink data transmissions on the traffic channel with a smaller CP (e.g., 25μs).

Once the access request message on a random access channel has been correctly decoded (i.e., the CRC checks), the access signal can be effectively used as the "preamble" for the device timing estimation after the message (known) is removed from the modulation symbols. Since the time offset Δt between the arrival time and the base station timing (due to round-trip propagation delay), Δt, of a random access signal causes phase-ramping in the received signal in the frequency domain at a rate proportional to the time offset, the time offset can be estimated from the phase difference between two modulation symbols, $\boldsymbol{y}_i$ and $\boldsymbol{y}_j$, on different subcarriers.

Since the carrier frequency offset Δf between the MTC device and the base station, i.e., the residual frequency synchronization error from the system acquisition causes a similar phase ramping effect on the received baseband signal in the time domain, we have

$$\begin{aligned}\boldsymbol{y}_j\boldsymbol{y}_i^* &= \left(he^{j2\pi\left(-q_jT^{-1}\Delta t+(T+T_{\rm CP})\Delta f\cdot j\right)}+\boldsymbol{v}_j\right)\\ &\quad\times\left(he^{j2\pi\left(-q_iT^{-1}\Delta t+(T+T_{\rm CP})\Delta f\cdot i\right)}+\boldsymbol{v}_i\right)^*\\ &= |h|^2\,e^{j2\pi\left((q_i-q_j)T^{-1}\Delta t+(T+T_{\rm CP})\Delta f(j-i)\right)}\\ &\quad+he^{j2\pi\left(-q_jT^{-1}\Delta t+(T+T_{\rm CP})\Delta f\cdot j\right)}\cdot\boldsymbol{v}_i^*\\ &\quad+h^*e^{-j2\pi\left(-q_iT^{-1}\Delta t+(T+T_{\rm CP})\Delta f\cdot i\right)}\boldsymbol{v}_j+\boldsymbol{v}_j\cdot\boldsymbol{v}_i^*\\ &= |h|^2\,e^{j2\pi\left(\Delta qT^{-1}\Delta t+(T+T_{\rm CP})\Delta f(j-i)\right)}+\boldsymbol{u}_{i,j},\end{aligned} \tag{11}$$

where h is the channel gain; q_i and q_j are the indices of subcarriers, which are occupied by symbol $\boldsymbol{y}_i$ and $\boldsymbol{y}_j$, $\Delta q \triangleq q_i - q_j$ is the separation (in subcarriers) between two modulation symbols, $T^{-1} = w_0$ is the subcarrier spacing of the OFDM symbol, $\boldsymbol{v}_i$ is the zero-mean Gaussian noise with variance σ^2, and $E\left\{\boldsymbol{v}_j\boldsymbol{v}_i^*\right\} = 0, \forall j \neq i$, and

$$\begin{aligned}\boldsymbol{u}_{i,j} &\triangleq he^{j2\pi\left(-q_jT^{-1}\Delta t+(T+T_{\rm CP})\Delta f\cdot j\right)}\cdot\boldsymbol{v}_i^*\\ &\quad+h^*e^{-j2\pi\left(-q_iT^{-1}\Delta t+(T+T_{\rm CP})\Delta f\cdot i\right)}\boldsymbol{v}_j+\boldsymbol{v}_j\boldsymbol{v}_i^*.\end{aligned} \tag{12}$$

It can be shown that $E\left\{\boldsymbol{u}_{i,j}\right\} = 0$. Therefore,

$$E\left\{\boldsymbol{y}_j\boldsymbol{y}_i^*\right\} = |h|^2\,e^{j2\pi\left(\Delta qT^{-1}\Delta t+(T+T_{\rm CP})\Delta f(j-i)\right)}. \tag{13}$$

Fig. 5 illustrates how an access request signal is mapped onto the physical random access channels to facilitate the time offset estimation, where we have groups of modulation symbols of a random access signal hopping between two physical random access channels to create a separation of $\Delta q \neq 0$ subcarriers between two groups of modulation symbols.

To estimate the time offset, the frequency offset in (13) is first obtained using the modulation symbols in a group on the same subcarrier, for which $\Delta q = 0$ [12], and

$$\Delta f = \frac{1}{2\pi\,(T + T_{\rm CP})}\arctan E\left\{\boldsymbol{y}_{i+1}\boldsymbol{y}_i^*\right\} \tag{14}$$

conditioned on

$$2\pi\cdot(T + T_{\rm CP})\,|\Delta f| < \pi. \tag{15}$$

Specifically, an estimate of (14) is

$$\Delta\hat{f} = \frac{1}{2\pi\,(T + T_{\rm CP})}\arctan\sum_{n=0}^{N_{\rm OFDM}/l-1}\sum_{k=0}^{l-2}\boldsymbol{y}_{n\cdot l+k+1}\boldsymbol{y}_{n\cdot l+k}^* \tag{16}$$

where l is the number of modulation symbols in one group.

After the temporal phase ramping is removed using the result from (16), the time offset is then obtained from the modulation symbols that are on separate subcarriers (i.e., $\Delta q > 0$), i.e.,

$$\Delta t = \frac{1}{2\pi T^{-1}\Delta q}\arctan E\left\{\boldsymbol{y}_i\boldsymbol{y}_{i+l}^*\right\}, \tag{17}$$

as long as

$$2\pi\,\Delta qT^{-1}\Delta t < 2\pi. \tag{18}$$

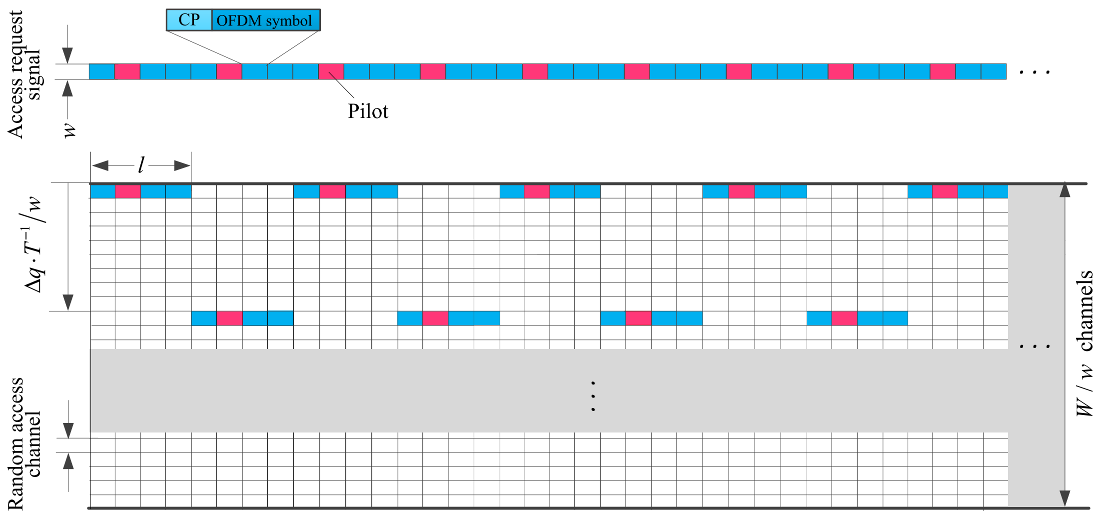

FIGURE 5. Illustration of access request signal hopping for time offset estimation.

TABLE 1. Transmission time intervals (TTIs) of the proposed packet-based preamble. EPA channel with 1Hz Doppler which is the typical channel condition in mIoT [13] is used and $S = 48$ subcarriers. The TTIs for legacy LTE random access signals at different random access stages (cf. Fig.2) are also included for reference. $W = 180$ kHz for proposed packet-based preamble, and $W = 1.08$ MHz for legacy LTE.

		TTI (sec)
Proposed	Tx1	0.245
LTE (LTE-eMTC)	Tx1	0.08
	Rx1	1.564
	Tx2	0.85
	Rx2	0.574
	Tx3	0.13

An estimate of (17) is

$$\Delta\hat{t} = \frac{1}{2\pi T^{-1}\Delta q} \arctan \sum_{n=0}^{N_{\mathrm{OFDM}}/2l-1} \times \left(\left(\sum_{k=0}^{l-1} \mathbf{y}'_{2l\cdot n+k} \right) \cdot \left(\sum_{k=0}^{l-1} \mathbf{y}'_{l(2n+1)+k} \right)^{*} \right) \quad (19)$$

where $\mathbf{y}'$ is the signal after removing the time-domain phase ramp caused by frequency offset. Clearly, a larger Δq corresponds to a smaller estimation error. From (18), the maximum value of Δq depends on the largest time offset Δt, which is the maximum round-trip propagation delay and a function of the cell size. For example, the maximum value of Δq is 7 for a 5-km radius cell at a subcarrier spacing of 3.75 kHz.

IV. SIMULATION RESULTS

Fig. 6 shows the link performance of the proposed packet-based preamble. The transmission time interval (TTI) for the access request preamble is 0.245 second. The TTIs for the legacy LTE random access signals are also listed in Table 1 for reference. The operating SNR Γ is calculated

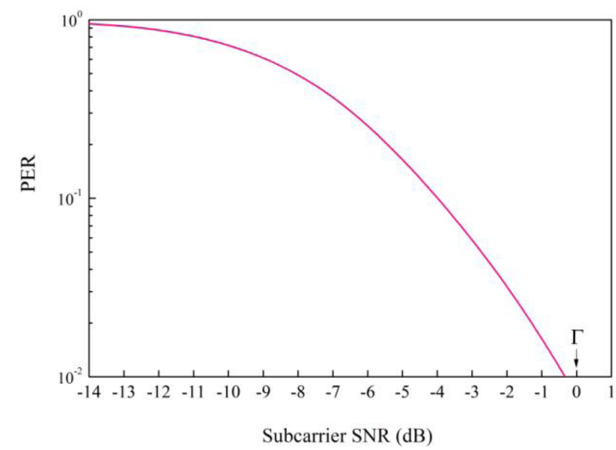

FIGURE 6. Decoding/detection performance (packet error rate or PER) of the proposed packet-based preamble at operating SNR Γ. The frequency offset is assumed to be uniformly-distributed in [−50, 50] Hz, and the time offset in [0, 35] μs. The total bandwidth is $W = 180$ kHz. The transmission time interval (TTIs) is determined to be 0.245 s to close the operation system. The TTI is the minimum transmission length determined such that the SNR at 1% packet error rate (PER) is less than Γ.

according to (4) as

$$\Gamma = p - \Delta - (N_0 + \eta + w) = 0 \text{ dB},$$

where $p = 20$ dBm is the device transmit power, $\Delta = 155$ dB is the maximum coupling loss (pathloss), $N_0 = -174$ dBm/Hz is the noise power spectral density, $\eta = 3$ dB is the noise figure of the receiver at the base station, and $w = 3.75$ KHz $= 35.7$ dB$\cdot$Hz is the transmission bandwidth.

After taking into account the collision and decoding error ($p_e = 1\%$), the average transmission time for mIoT is

$$t_{\mathrm{Tx}} = \frac{T_{\mathrm{Tx}}}{(1-p_c)(1-p_e)} = \frac{0.245 \text{ sec}}{(1-9\%)(1-1\%)} \approx 0.27 \text{ sec} \quad (20)$$

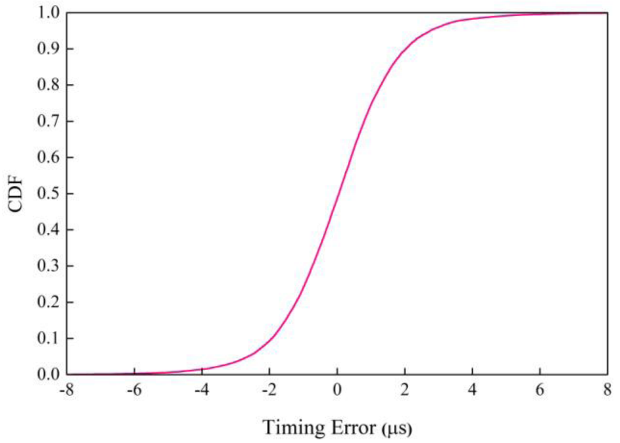

FIGURE 7. **Timing estimation performance of the packet-based access request signal with operating SNR Γ. The frequency offset is assumed to be uniformly-distributed in [−50, 50] Hz, and the time offset in [0, 35] μs.**

where T_{Tx} is the TTI for the packet-based preamble and 9% collision probability. Hence, the battery consumption per random access is

$$C_{\text{LTE-nMTC}} = t_{\mathrm{Tx}} I_{\mathrm{Tx}} = 0.27\,\text{sec} \times 260\text{mA} \approx 0.020\text{mAh} \tag{21}$$

or 0.0004% of the capacity of two AA batteries (C_{AA} = 5000mAh).

For legacy LTE, it is approximately (ignoring the collision, miss of preamble detection, and random access response and contention resolution decoding error)

$$\begin{aligned} C_{\text{LTE-eMTC}} &= t_{\mathrm{Tx}} I_{\mathrm{Tx}} + t_{\mathrm{Rx}} I_{\mathrm{Rx}} = (T_{\mathrm{Tx1}} + T_{\mathrm{Tx2}} + T_{\mathrm{Tx3}})\, I_{\mathrm{Tx}} \\ &\quad + (T_{\mathrm{Rx1}} + T_{\mathrm{Rx2}})\, I_{\mathrm{Rx}} \\ &= (0.08 + 0.85 + 0.13)\,\text{sec} \times 260\text{mA} \\ &\quad + (1.564 + 0.574)\,\text{sec} \times 150\text{mA} \\ &\approx 0.166\text{mAh} \end{aligned} \tag{22}$$

or 0.0033% of the capacity of two AA batteries. This is an 88% reduction in battery consumption for each random access.

Fig. 7 shows the timing estimation performance using the proposed packet-based preamble. We observe that the timing error is in the range of $\pm 5\mu$s (95 percentile), which consumes approximately 10μs of the CP, leaving 15μs for the multipath delay spread, which is sufficient for the traffic channels.

V. CONCLUSION

The random access procedure in the legacy LTE system is optimized for human-type communication, which is not suitable for the massive IoT because of the large battery consumption which is caused by the sequence of handshakes process that followed the preamble detection. We simplify the random access process by replacing the ZC sequence-based preamble CDMA signal with a special OFDM signal to negate the need for the preamble, contention resolution, and conventional threshold-based waveform detection. The power consumption analyses show an over 88% reduction in battery consumption compared to the traditional LTE random access. The timing estimation performance of our proposed packet-based preamble also works well and is sufficient for the traffic channels with the shortened CP. We also analyze the effect of the transmission bandwidth on the transmission time and system capacity, and we use the suboptimal transmission bandwidth in our packet-based preamble design to achieve high power and spectral efficiency.

REFERENCES

[1] H. Chaouchi, *The Internet of Things: Connecting Objects to the Web*. Hoboken, NJ, USA: Wiley, 2010.
[2] S. M. R. Islam, D. Kwak, M. H. Kabir, M. Hossain, and K.-S. Kwak, "The Internet of Things for health care: A comprehensive survey," *IEEE Access*, vol. 3, pp. 678–708, Jun. 2015.
[3] M. Wang *et al.*, "Cellular machine-type communications: Physical challenges and solutions," *IEEE Wireless Commun.*, vol. 23, no. 2, pp. 126–135, Apr. 2016.
[4] T. N. Pham, M.-F. Tsai, D. B. Nguyen, C.-R. Dow, and D.-J. Deng, "A cloud-based smart-parking system based on Internet-of-Things technologies," *IEEE Access*, vol. 3, pp. 1581–1591, 2015.
[5] Z. Dawy, W. Saad, A. Ghosh, J. G. Andrews, and E. Yaacoub, "Toward massive machine type cellular communications," *IEEE Wireless Commun.*, vol. 24, no. 1, pp. 120–128, Feb. 2017.
[6] A. Gupta and R. K. Jha, "A survey of 5G network: Architecture and emerging technologies," *IEEE Access*, vol. 3, pp. 1206–1232, 2015.
[7] *Services and System Aspects System Improvements for Machine-Type Communications (MTC) (Release 11)*, Doc. TS 23.888 v11.0.0, 3GPP, Sep. 2012.
[8] *Radio Access Network Evolved Universal Terrestrial Radio Access (E-UTRA) Physical Channels and Modulation (Release 13)*, Doc. TS 36.211, 3GPP, 2016.
[9] M. Hua *et al.*, "Analysis of the frequency offset effect on random access signals," *IEEE Trans. Commun.*, vol. 61, no. 11, pp. 4728–4740, Nov. 2013.
[10] M. Hua, M. Wang, K. W. Yang, and K. J. Zou, "Analysis of frequency offset effect on Zadoff–Chu sequence timing performance," *IEEE Trans. Commun.*, vol. 62, no. 11, pp. 4024–4039, Nov. 2014.
[11] S. Ye, S. H. Wong, and C. Worrall, "Enhanced physical downlink control channel in LTE advanced release 11," *IEEE Commun. Mag.*, vol. 51, no. 2, pp. 82–89, Feb. 2013.
[12] T. Brown and M. M. Wang, "An iterative algorithm for single-frequency estimation," *IEEE Trans. Signal Process.*, vol. 50, no. 11, pp. 2671–2682, Nov. 2002.
[13] *Radio Access Network Evolved Universal Terrestrial Radio Access (E-UTRA) User Equipment (UE) Radio Transmission and Reception (Release 11)*, Doc. TS 25.996 ver.11.0.0, 3GPP, Sep. 2012.

JUN ZOU received the Ph.D. degree from the Wireless Networking and Mobile Communications Group, School of Electronic and Optical Engineering, Nanjing University of Science and Technology, Nanjing, China. Since 2016, he has been with the Wireless Networking and Mobile Communications Group, Nanjing University of Science and Technology, where he is currently a Lecturer with the School of Electronic and Optical Engineering. He has authored or co-authored over ten IEEE journal publications. His research interests are in the areas of wireless communications, signal processing, and Internet of Things.

HAI YU is currently pursuing the Ph.D. degree at the Wireless Networking and Mobile Communications Group, School of Electronic and Optical Engineering, Nanjing University of Science and Technology, Nanjing, China. His research interests are in the areas of wireless communications and signal processing.

WEIWEI MIAO received the M.S. degree from the School of Automation, Southeast University, Nanjing, China. Since 1992, he has been with the State Grid Jiangsu Electric Power Company, Nanjing, China, where he is currently the Principal Expert for power communication in Jiangsu, China. His research interests are in the areas of power wireless private network and the applications of wireless and wired communication in grid and hybrid networking technology.

CHENGLING JIANG received the Ph.D. degree from the School of Electronic and Optical Engineering, Nanjing University of Science and Technology, Nanjing, China. Since 2013, he has been with the Information and Telecommunication Branch, State Grid Jiangsu Electric Power Company, Nanjing. His research interests are in the areas of wireless communications and power wireless private networks.