
Low Latency Signature-Based 4-Step Random Access Procedure for Massive Machine-Type Communications

Wei-Chieh Wang, Yao-Jen Liang, Hwang-Cheng Wang,
Fang-Chang Kuo and Chih-Cheng Tseng*

*No.1, Sec. 1, Shennong Rd., Yilan City, Yilan County 260, Taiwan (R.O.C.)
E-mail: rwe587360@gmail.com; yaojen@niu.edu.tw; hcwang@niu.edu.tw;
kfc@niu.edu.tw; tsengcc@niu.edu.tw*

**Corresponding Author*

Received 11 March 2023; Accepted 11 September 2023;
Publication 07 February 2024

Abstract

Massive machine-type communication (mMTC) is one of the major services in the 5G new radio (NR) system. In the mMTC application scenarios, many machine-type communication devices (MTCDs) communicate with each other or through an MTC server. However, how to solve the problem of excessive MTCDs accessing the network simultaneously is an important task. To overcome the large number of random access collisions and retransmission problems, this paper proposes a method to solve the mMTC random access problem. The proposed method consists of two parts, modified Contention Based Random Access (CBRA) with 4-step RA type and 4-step Signature RA type. With the modified CBRA with 4-step RA type, each MTCD will obtain the information to generate the signature. After that, the 4-step Signature RA type is used for MTCDs to proceed with the random access with the gNB through the generated signatures. In our proposed method, the average number of false positives and average process time are evaluated under

Journal of Mobile Multimedia, Vol. 20_1, 23–48.

doi: 10.13052/jmm1550-4646.2012

© 2024 River Publishers

different numbers of active MTCDs and different parameter values for the signature generation. Besides, the average number of preamble attempts and average process time are used as the metrics to compare the proposed scheme with the 5G NR 4-step RA type. Finally, simulation results show that the proposed scheme performs better than the 5G NR 4-step RA type in the mMTC scenarios.

Keywords: mMTC, 5G new radio (NR), contention based random access (CBRA), MTCDs, signature.

1 Introduction

In the research report M.2410-0 [1], ITU-R (International Telecommunication Union-Radiocommunication Sector) proposed three major application scenarios for IMT-2020: eMBB (enhanced mobile broadband), URLLC (ultra-reliable and low-latency communications), and mMTC (massive machine-type communications). In [2], 3GPP delivered some service requirements and practical applications for MTC. For the mMTC application scenario, the connection density would be probably greater than 10^6 devices/km². Besides, the devices are with the properties of small volume of data transmission, low energy consumption, long battery life, and the functions of sensing and tracking. For example, the smart meters in a smart city, the intelligent appliances in the smart Internet of Things, and the damage detection devices in the environment surveillance.

1.1 Random Access Procedure (RAP)

In current mobile telecommunication systems, User Equipment (UE) needs to proceed with the random access procedure (RAP) to establish an initial connection with the gNB and obtain the uplink (UL) radio resource allocation information for the upcoming UL transmissions. In Section 9.2.6 of [3], the reasons for UE to trigger the RAP are: (i) initial access from RRC_IDLE, (ii) radio resource control (RRC) connection re-establishment procedure, (iii) downlink (DL) or UL data arrival during RRC_CONNECTED or during RRC_INACTIVE while small data transmission (SDT) procedure is ongoing, when UL synchronization status is “non-synchronized”, (iv) UL data arrival during RRC_CONNECTED or during RRC_INACTIVE while SDT procedure is ongoing, when there is no physical uplink control channel (PUCCH) resource for scheduling request (SR) available, (v) SR failure,

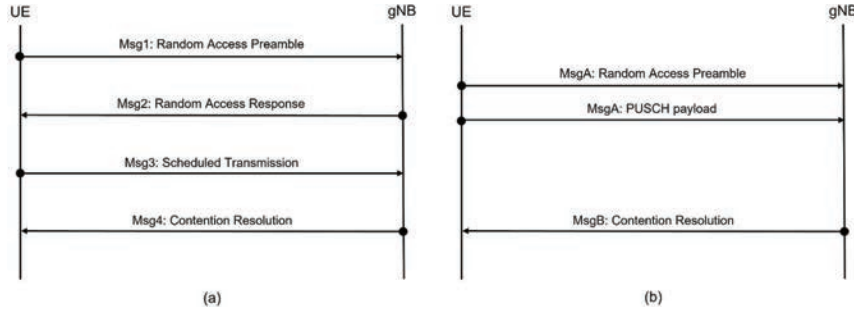


Figure 1 Contention-based RAP: (a) 4-step RA type and (b) 2-step RA type.

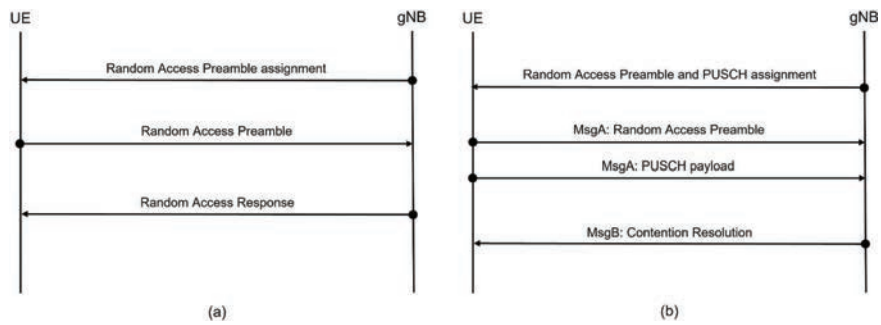


Figure 2 Contention-free RAP: (a) 4-step RA type and (b) 2-step RA type.

(vi) request by RRC upon synchronous reconfiguration (e.g., handover), (vii) RRC connection resume procedure from RRC_INACTIVE, (viii) establish time alignment for a secondary timing advance group (TAG), (ix) request for other system information (SI), (x) beam failure recovery, (xi) consistent UL listen before talk (LBT) failure on special cell (SpCell), (xii) SDT in RRC_INACTIVE, (xiii) positioning purpose during RRC_CONNECTED requiring random access procedure (e.g., when timing advance is needed for UE positioning). In general, the random access (RA) modes can be classified into contention-based random access (CBRA) and contention-free random access (CFRA). The types of RAP supported by the 5G New Radio (NR) are 4-step RA type and 2-step RA type. Besides, both types support CBRA and CFRA modes. Figures 1 and 2 demonstrate the operations of 4-step RA type and 2-step RA type in the CBRA and CFRA modes, respectively [3].

The selection of RA type for UE is based on the following three network allocations: (i) when the resource of CFRA is not configured, a threshold for the reference signal received power (RSRP) is used by the UE to select

the 2-step RA type or 4-step RA type; (ii) when the network resource of the CFRA for 4-step RA type is configured, UE uses the 4-step RA type to perform the RA; (iii) when the network resource of the 2-step RA type is configured, UE uses the 2-step RA type to perform the RA. Some exemplified designs of CBRA 2-step RA type design can be found in [4, 5].

1.2 CBRA 4-step Random Access Type

When UE selects the CBRA 4-step RA type, the 4-step RAP is used to establish a radio resources connection. The detailed contention procedure of the CBRA 4-step RA type is as below [6]:

- Step1 (Msg1: Random Access Preamble): At the beginning, UE obtains the allocation of the random access channel (RACH) from the system information (SI) broadcast from the gNB. Based on the received SI, UE generates 64 preambles. On the allocated random access opportunity (RAO), UE randomly selects a preamble and sends it to the gNB. Then, UE waits for the downlink control information (DCI) and random access response (RAR) from the gNB within the following *ra-ResponseWindow*.
- Step2 (Msg2: Random Access Response, RAR): After gNB correctly received and decoded the preamble from the UE, it generates the RAR based on the radio resource that UE used to send the preamble and the decoded RAPID (random access preamble identifier). The RAR consists of Timing Advance Command, UL Grant, and Temporary Cell Radio Network Temporary Identifier (TC-RNTI).
- Step3 (Msg3: Scheduled Transmission): After successfully decoding the received RAR, UE sends the Msg3 on the physical uplink shared channel (PUSCH) to gNB and initiates the *ra-ContentionResolutionTimer* to wait for the Msg4 sent from gNB. If UE already has the Cell-RNTI (C-RNTI), the content of Msg3 is C-RNTI MAC CE. Otherwise, UE sends the 48-bit UE Contention Resolution Identity MAC CE that consists of ue-Identity, establishmentCause, and spare bits.
- Step4 (Msg4: Contention Resolution): After successfully decoded Msg3, gNB responses UE the Msg4 on the physical downlink control channel (PDCCH). The Msg4 contains 48-bit UE Contention Resolution Identity MAC CE from the received Msg3. Hence, after Msg4 is received, UE checks if the contents of the UE Contention Resolution Identity MAC CEs are the same as the ones it sent in Msg3. If yes, UE stops the *ContentionResolutionTimer*, sets the value of C-RNTI to the

value of TC-RNTI that is received in Msg2, and drops the TC-RNTI. Otherwise, UE drops the TC-RNTI and the decoded MAC PDU and regards the Contention Resolution a fail.

When massive MTCs proceed RAP for initial access to gNB simultaneously, due to the limited radio resources, a great number of collisions occur among MTCs resulting in the increase of the time and energy consumption required to complete the RAP. To decrease the radio access network (RAN) overhead in the MTC application scenarios, the following approaches are proposed by 3GPP in [7]: (i) Access Class Barring (ACB) schemes, (ii) Separate RACH resources for MTC, (iii) Dynamic allocation of RACH resources, (iv) MTC Specific Backoff scheme, (v) Slotted access, and (vi) Pull based scheme. The two commonly used ACB schemes are UE individual Access Class Barring Scaling and Extended Access Barring. In the UE individual Access Class Barring Scaling scheme, the parameters for access control are managed by the base station and broadcast to the individual UE or a group of UEs. In the Extended Access Barring scheme, UEs that can tolerate the access control are configured as the EAB-configurable UE. As the network traffic is overloaded, gNB adaptively and selectively limits the access attempts of the EAB-configured UEs. Normally, the MTC and human to human (H2H) communications share the same RACH. Hence, they may collide during the RAP. In the separate RACH resources for MTC scheme, the RACH resources are split exclusively for MTC and H2H. In the application scenarios where the traffic load from the MTC is predictable, gNB may dynamically adapt the RACH resources to reduce the random access collision. The concept to reduce the random access collision in the MTC specific backoff scheme is to defer the re-attempts of the MTCs by adapting the backoff time. By doing so, the retransmission times of the MTCs are interleaved. In the slotted access scheme, the random access collision is prevented by allocating each MTC with a unique slot based on its International Mobile Subscriber Identity (IMSI). Each MTC can only proceed with the RAP on its allocated slot. In the pull-based scheme, an MTC server is introduced with the knowledge of when each MTC wants to do the UL transmission, Hence, MTC proceeds with the RRC-connection establishment after being paged by the gNB. This scheme is also applicable to the transmission between an MTC and the core network. Based on the load estimation model, the authors in [8] improved the access successful probability and average access delay by adjusting the ACB parameters based on the results from the load estimation model. In [9, 10], the concept of signature was utilized to expand

the varieties of preambles, thus the signal overhead and the re-attempt times of the RAP in the MTC application scenarios can be reduced. To reduce the random access collision probability and the latency of the 4-step RAP, this paper proposes a modified CBRA with 4-step RA type and 4-step Signature RA type. The modified CBRA with 4-step RA type is used to obtain the information required to generate the signature for each individual MTC. After that, the 4-step Signature RA type is used for MTCs to establish the RRC connections.

This paper is organized as follows. The system model is described in Section 2. Section 3 is the detail design of the proposed modified CBRA with 4-step RA type and 4-step Signature RA type. Simulation results are presented in Section 4. Finally, Section 5 concludes this paper.

2 System Model

Under CBRA with 4-step RA type, the RAP is regarded a failure if any of the following two situations occurred [11]: (i) If UE does not receive the RAR from gNB before *ra-ResponseWindow* expires, UE triggers the retransmission mechanism and increase the value of *PREAMBLE_TRANSMISSION_COUNTER* by one. If the number of retransmissions exceeds the preconfigured upper limit, *preambleTransMax*, the RAP is regarded a failure. (ii) If more than one UE sends the same preamble in the same RAO, multiple Msg3s collide due to the UEs are assigned with the same uplink radio resource. In this case, each collided UE based on the value of Backoff Indicator in the MAC subPDU of RAR to configure the backoff time. After the backoff time expires, the collide UE starts the RAP from Step1. If the value of the counter for the number of preamble transmissions, *PREAMBLE_TRANSMISSION_COUNTER*, exceeds the upper limit, the RAP is regarded a failure. Among the above two situations, due to the massive number of MTCs, situation (ii) occurs frequently resulting in a large number of MTCs keep proceeding with the RAP. Consequently, not only the battery power of MTCs and the limited radio resources are wasted, but the time to complete the RAP is also increased dramatically.

To reduce the occurrence of situation (ii) in the mMTC application scenarios, the random access preamble and RAR are re-designed based on the concept of signature. Besides, to simplify our design, the impacts from the physical layer, e.g., the incorrect reception and decoding due to the imperfect channel, are not considered.

2.1 System Model

The considered system model is depicted in Figure 3, wherein there are one gNB and C MTCDs. All the MTCDs follow the procedures of CBRA with 4-step RA type to perform the random access. In each round of contention, the state of each MTCD is either active or inactive. The number of active and inactive MTCDs are C_{active} and $C_{inactive}$, respectively.

2.2 Radio Resource Control

In 5G NR, the RRC states are defined as RRC_IDLE, RRC_INACTIVE, and RRC_CONNECTED [12]. In addition to the two RRC states, (RRC_IDLE and RRC_CONNECTED), defined in LTE, RRC_INACTIVE state is added in 5G NR to reduce the transition time for UE from the RRC_IDLE to RRC_CONNECTED, as shown in Figure 4. It should be noted that

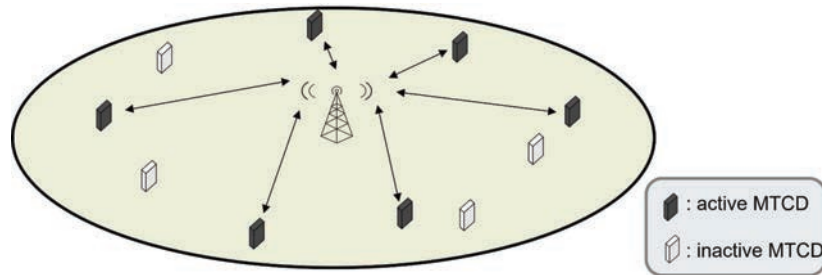


Figure 3 System model.

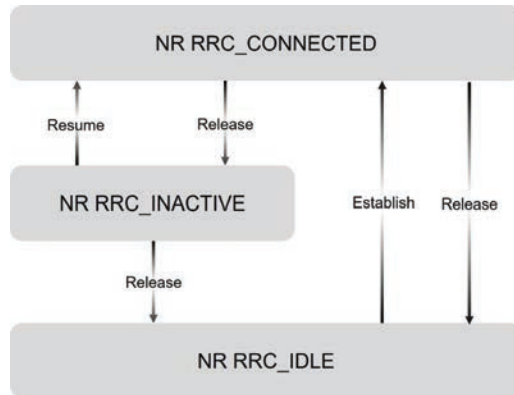


Figure 4 RRC states in NR.

data payload transmission only occurs between the RRC_IDLE and RRC_CONNECTED states to meet the characteristics of low data rate and high delay tolerance of massive MTCDs.

3 4-step Signature RA Type

To improve the collision due to different MTCDs transmitting the same preamble in the same RAO [9, 10], inspired by the Bloom filter, the concept of signature is applied to increase the number of possible preamble combinations in the time domain. Specifically, the idea of subscriber key (SK) and random challenge are combined to generate the signature in [9]. Besides, MTCD and gNB both obtain the information of SK from the home subscriber server (HSS) for the generation and the verification of signature, respectively. As depicted in Figure 5, the proposed 4-step Signature RA type differs from the CBRA with 4-step RA type in the Step1 and Step2.

3.1 Modified CBRA with 4-step RA Type

To obtain the required information for generating the signature, a newly deployed MTCD for accessing the network is required to follow the procedures of the modified CBRA with 4-step RA type, as shown in Figure 6. In the beginning, each newly deployed MTCD decodes the system information block 1 (SIB1) from the gNB to obtain all the required information for

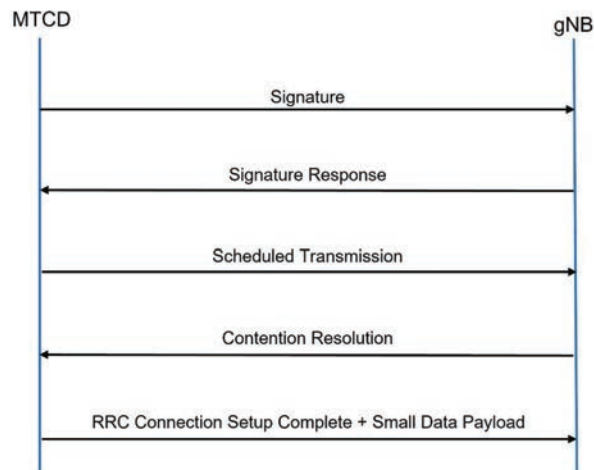


Figure 5 4-step signature RA type.

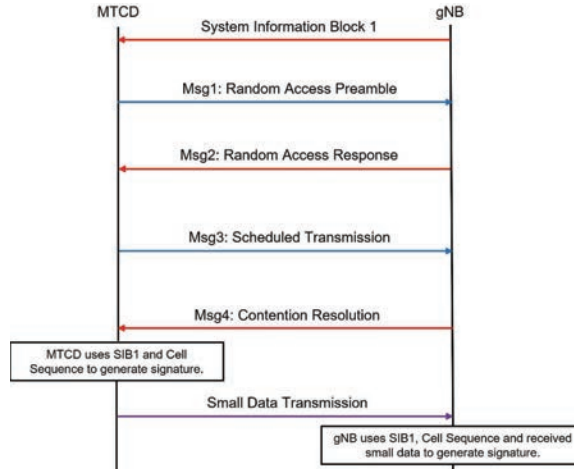


Figure 6 The modified CBRA with 4-step RA type.

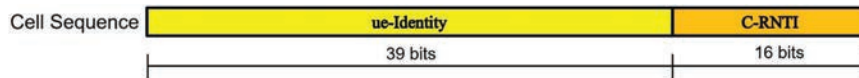


Figure 7 Cell sequence.

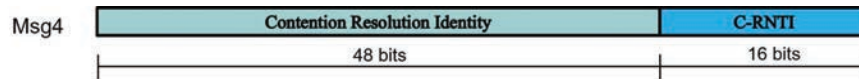


Figure 8 Contention resolution.

accessing the network. In particular, we introduce the total number of RAOs consists of a signature, L , and the number of RAOs, K used for designing the preambles. The key modification of the CBRA with 4-step RA type is that after receiving the Msg3, gNB assigns the value of TC-RNTI is generated in Msg2 to C-RNTI and then, combines C-RNTI and the received ue-Identity to generate the cell sequence as illustrated in Figure 7. Next, by comparing all the cell sequences in the Cell Sequence Table, gNB checks if the generated cell sequence is a new one. If yes, it will be stored in the Cell Sequence Table. Otherwise, gNB generates a new C-RNTI that has not been used to replace the old one and stores the updated cell sequence in the Cell Sequence Table. Next, as shown in Figure 8, gNB integrates the Contention Resolution Identity and the C-RNTI to generate the Msg4 (or Contention Resolution). Based on the C-RNTI in the received Msg4, the MTC regenerates the cell sequence. By using the regenerated cell sequence and the parameters in the

received SIB1, MTCB generates its own signature and sends the identifiers of the randomly selected preambles in each of the K RAOs to the gNB. After receiving the K preamble identifiers, gNB generates the signature of the MTCB and stores it in the Signature Table. Eventually, the Cell Sequence Table and Signature Table will contain cell sequences and signatures of all the C MTCBs, respectively. All the operations mentioned above will be detailed explained in the following subsections.

3.2 Signature Generation

In our design, a hash function is used to generate the signature. The inputs to the hash function are the number of RAOs consisting of a signature L , the number of RAOs that are used to send preamble K , and Cell Sequence. The signature of MTCB l is represented as

$$\mathbf{s}^l = \begin{bmatrix} s_{1,1}^l & \cdots & s_{1,L}^l \\ \vdots & \ddots & \vdots \\ s_{M,1}^l & \cdots & s_{M,L}^l \end{bmatrix} = [\mathbf{s}_1^l \mathbf{s}_2^l \cdots \mathbf{s}_j^l \cdots \mathbf{s}_L^l], \quad (1)$$

where $\mathbf{s}_j^l = [s_{1,j}^l \ s_{2,j}^l \ \cdots \ s_{i,j}^l \ \cdots \ s_{M,j}^l]^T$, $i = 1, \dots, M$, $j = 1, \dots, L$, and $s_{i,j}^l = 1$ if the i -th preamble is sent in the j -th RAO; otherwise, $s_{i,j}^l = 0$. In each RAO j , at most one preamble is sent, i.e., $|\mathbf{s}_j^l| = \sum_{i=1}^M s_{i,j}^l \leq 1$. Besides, only K out of L RAOs can be used to send the preamble, i.e., $\sum_{j=1}^L |\mathbf{s}_j^l| = K$.

Among the L RAOs, the selection of the K out of L RAOs to send the preamble is based on the double hashing mechanism in (2), (3), and (4).

$$h_1(D_{CS}^l) = D_{CS}^l \bmod L \quad (2)$$

$$h_2(D_{CS}^l) = 1 + (D_{CS}^l \bmod (L - 1)) \quad (3)$$

$$h(D_{CS}^l, k) = (h_1(D_{CS}^l) + kh_2(D_{CS}^l)) \bmod L \quad (4)$$

where D_{CS}^l is the cell sequence of MTCB l and $k = 1, \dots, K$. Besides, to meet the double hashing mechanism, L must be a prime. The steps to generate the signature of MTCB l are as follows:

Step 1: Based on the double hashing mechanism in (2), (3), and (4) to determine the K RAOs to send the preamble.

Step 2: In each determined RAO, randomly select a preamble among the M available preambles.

Please note that, as mentioned in Section 3.1, the generation of signature for each MTCD is only done when the MTCD first time accesses to the network. After that, the generated signature is used for MTCD to perform the 4-step Signature RA type.

3.3 Cell Sequence Table and Signature Table

Following the procedures of the modified CBRA with 4-step RA type in Section 3.1 and the steps to generate the signature in Section 3.2, the Cell Sequence Table and Signature Table maintained in the gNB are shown in Figures 9 and 10, respectively.

3.4 Signature Transmission and Reception

The transmission of the signature for the MTCD and the reception of the signature for the gNB are discussed in this subsection.

$$\begin{aligned}
 D_{CS}^1 &= 10001010001\dots \\
 D_{CS}^2 &= 01101011101\dots \\
 D_{CS}^3 &= 11110001101\dots \\
 &\vdots \\
 D_{CS}^{C-1} &= 01001110100\dots \\
 D_{CS}^C &= 01011111100\dots
 \end{aligned}$$

Figure 9 Cell Sequence Table.

$$\begin{aligned}
 \mathbf{S}^1 &= [\mathbf{s}_1^1 \ \mathbf{s}_2^1 \dots \mathbf{s}_j^1 \dots \mathbf{s}_L^1] \\
 \mathbf{S}^2 &= [\mathbf{s}_1^2 \ \mathbf{s}_2^2 \dots \mathbf{s}_j^2 \dots \mathbf{s}_L^2] \\
 \mathbf{S}^3 &= [\mathbf{s}_1^3 \ \mathbf{s}_2^3 \dots \mathbf{s}_j^3 \dots \mathbf{s}_L^3] \\
 &\vdots \\
 \mathbf{S}^{C-1} &= [\mathbf{s}_1^{C-1} \ \mathbf{s}_2^{C-1} \dots \mathbf{s}_j^{C-1} \dots \mathbf{s}_L^{C-1}] \\
 \mathbf{S}^C &= [\mathbf{s}_1^C \ \mathbf{s}_2^C \dots \mathbf{s}_j^C \dots \mathbf{s}_L^C]
 \end{aligned}$$

Figure 10 Signature Table.

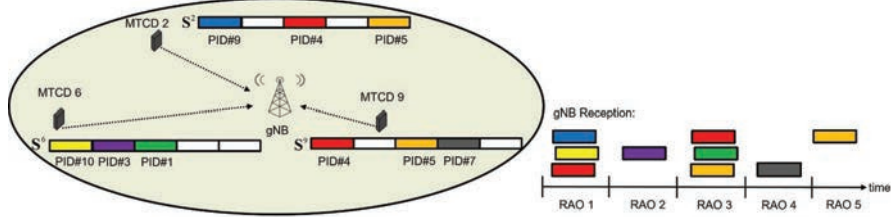


Figure 11 Example of signature transmission and reception.

- **Transmission:** After the signature is generated, it will be used by an MTCD in the first step of the 4-step Signature RA type. As illustrated in Figure 11, an example for $L = 5$, $K = 3$, and $M = 10$ is used to demonstrate the operations for the three active MTCDs, 2, 6, 9, to send their signatures. In this example, the signatures for these 3 active MTCDs are given in (5) and are sent to the gNB.

$$\begin{aligned}
 \mathbf{S}^2 &= \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \quad \mathbf{S}^6 = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{bmatrix}, \\
 \mathbf{S}^9 &= \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}. \tag{5}
 \end{aligned}$$

- Reception: Due to the orthogonal property of the preamble, after receiving all the preambles sent from the active MTCDS in each of the L RAOs, the received signature in gNB is given in (6)

$$\begin{bmatrix} y_{1,1} & \cdots & y_{1,L} \\ \vdots & \ddots & \vdots \\ y_{M,1} & \cdots & y_{M,L} \end{bmatrix} = \bigoplus_{r=1}^{C_{active}} \begin{bmatrix} s_{1,1}^{d_r} & \cdots & s_{1,L}^{d_r} \\ \vdots & \ddots & \vdots \\ s_{M,1}^{d_r} & \cdots & s_{M,L}^{d_r} \end{bmatrix}, \quad (6)$$

where \oplus is the bitwise OR operation, C_{active} is the number of active MTCDS, r is the index of the active MTCDS, and d_r is the index of the r -th MTCDS among the C MTCDS. For example, in Figure 11, $d_1 = 2$, $d_2 = 6$, and $d_3 = 9$. Let \mathbf{Y} and \mathbf{S}^{d_r} represent the matrices in the left and right-hand side of (6), respectively. Then, (6) can be simplified into (7)

$$\mathbf{Y} = \bigoplus_{r=1}^{C_{active}} \mathbf{S}^{d_r}. \quad (7)$$

3.5 Signature Decoding

After receiving \mathbf{Y} , gNB starts to decode the MTCDS that send the signatures. To do so, the gNB performs the bitwise AND operation between \mathbf{Y} and each of the signature \mathbf{S}^l in the Signature Table where $l = 1, \dots, C$. As in (8), if the result of the bitwise AND operation equals \mathbf{S}^l , MTCDS l is regarded as the MTCDS that sends the signature for the random access.

$$\mathbf{S}^l = \mathbf{S}^l \otimes \mathbf{Y} \quad (8)$$

Figure 12 shows the examples for gNB to decode the MTCDS under the assumptions of $L = 3$, $K = 3$, and $M = 10$. The signature received by gNB

$$\mathbf{Y} = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix} \quad \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \otimes \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix} \quad \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix} \otimes \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix} \quad \dots \quad \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix} \otimes \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}$$

Figure 12 Example of signature table decoding.

\mathbf{Y} is shown on the leftmost side of Figure 12. Then, gNB starts the bitwise AND operations between the received \mathbf{Y} and the signatures $\mathbf{S}^1, \mathbf{S}^2, \dots, \mathbf{S}^C$ in the Signature Table. As shown in Figure 12, MTCD 2 is identified as the MTCD that wants to access to the gNB.

Let D_t be the number of decoded signatures as given by

$$D_t = C_{active} + D_{FP}, \quad (9)$$

where D_{FP} is the number of false positives (i.e., a decoded signature that is not sent by the corresponding MTCD). Hence, when $D_t = C_{active}$, all the signatures sent by the C_{active} MTCDs are successfully decoded by the gNB and there is no decoded false positive. On the contrary, if $D_t > C_{active}$, in addition to signatures of the C_{active} MTCDs are successfully decoded, there are D_{FP} unsent signatures falsely decoded.

3.6 Signature Response (SR)

As described in [11], possible formats of subPDU inside the MAC PDU of RAR are as follows:

- A subheader carries the BI (backoff information).
- A subheader carries RAPID information.
- A subheader carries RAPID information followed by a payload that carries the MAC RAR.

In the proposed design, each SR is used to notify an MTCD with the decoded signature and the information about the allocated uplink radio resource. Each SR is encapsulated in a MAC subPDU and consists of a subheader and a payload. However, since the designed signature comprises multiple preambles, the BI and the RAPID defined in the 5G NR 4-step RA type are not used in the subheader of the proposed SR. Instead, to identify different MTCDs, the E/Cell Sequence information is carried in the subheader of the proposed SR as shown in Figure 13. The bit ‘E’ is used to indicate if this subPDU is the last one. Specifically, if $E = 0$, this subPDU is the last subPDU of the MAC PDU. Otherwise, it is followed by another subPDU.

However, in the proposed design, the format of the payload of SR remains the same as the one defined in the 5G NR 4-step RA type. That is, as shown in Figure 14, the payload is composed of Reserved bit, Timing Advance Command, UL Grant, and TC-RNTI. Hence, the MAC PDU in the proposed design is depicted in Figure 15.

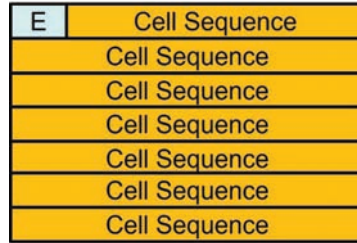


Figure 13 E/Cell sequence MAC SR subheader.

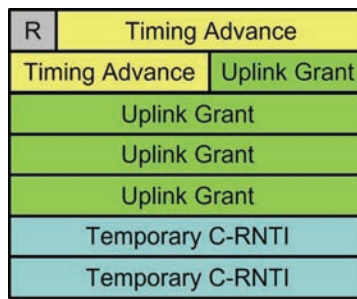


Figure 14 MAC SR payload.

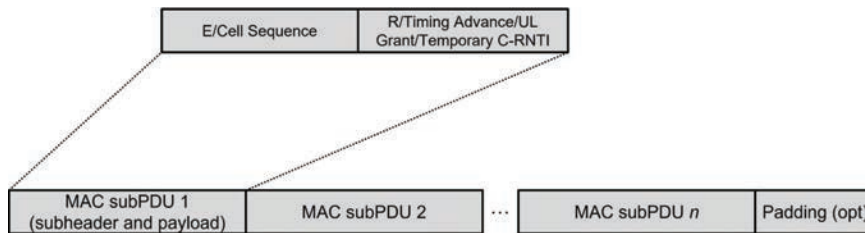


Figure 15 MAC PDU consisting of MAC subPDUs.

4 Simulation Results

In this section, the performance of the proposed 4-step Signature RA type is compared with that of the 5G NR 4-step RA type. Both the proposed 4-step Signature RA type and the 5G NR 4-step RA type are implemented in MATLAB. The Monte Carlo simulation is used to average the results collected in 100 simulations. Tables 1 and 2 are the parameter values used in the simulations for the proposed 4-step Signature RA type and the 5G NR 4-step RA type, respectively [11, 12]. To focus the attention mainly on the performance of the proposed design, the assumptions made in the simulations

Table 1 Parameter values for the 5G NR 4-step RA type

Parameter	Value
The time for transmitting Msg1, T_{Msg1}	1 ms
The time for transmitting Msg2, T_{Msg2}	1 ms
The time for transmitting Msg3, T_{Msg3}	3 ms
The time for transmitting Msg4, T_{Msg4}	3 ms
The processing time for decoding Msg1 and preparing Msg2, $T_{1.2}$	2 ms
The processing time for decoding Msg2 and preparing Msg3, $T_{2.3}$	2 ms
The processing time for decoding Msg3 and preparing Msg4, $T_{3.4}$	2 ms
The number of available preamble, M	54
The time period of a RAO, T_{RAO}	1 ms
The Backoff parameter value	5 ms
The Contention Resolution Timer, <i>re-ContentionResolutionTimer</i>	8 ms

Table 2 Parameter values for the proposed 4-step Signature RA type

Parameter	Value
The number of MTCDs in system model, C	1000
The number of active MTCDs in system model, C_{active}	(50~300), (100~900)
The number of available preamble, M	54
The number of RAOs per signature, L	(23, 53, 83)
The number of RAOs that are selected to transmit the preamble, K	(3, 4, 6, 9)
The time period of a RAO, T_{RAO}	1 ms
The time for transmitting Scheduled Transmission, T_{ST}	3 ms
The time for transmitting Contention Resolution, T_{CR}	3 ms
The processing time for decoding the signature and preparing SR, $T_{\text{S.SR}}$	2 ms
The processing time for decoding SR and preparing ST, $T_{\text{SR.ST}}$	2 ms
The processing time for decoding ST and preparing CR, $T_{\text{ST.CR}}$	2 ms

are (i) gNB only processes the random access requests from the active MTCDs; (ii) impacts due to the imperfection of wireless channel are ignored so that any unrecognized signal is from the transmissions of multiple active MTCDs over the same radio resources; (iii) all the considered active MTCDs perform the RAP simultaneously.

When the 5G NR 4-step RA type is considered, based on the parameter values in Table 1, each active MTCD randomly selects a preamble from the 54 available preambles and sends the selected preambles to gNB on the same RAO. However, only the MTCDs whose selected preambles are unique to others' may complete the whole RAP. For each of the active MTCDs whose selected preamble is not unique, it restarts the whole procedure after waiting

for *ra-ContentionResolutionTimer*. Since there is no limit for MTCDs to retry, the whole procedures of the 5G NR 4-step RA type will continue until the last active MTCD successfully completes the 5G NR 4-step RA type.

When the 4-step Signature RA type is considered, as mentioned in Sections 3.1, 3.2, and 3.3, the Cell Sequence Table and Signature Table for the C MTCDs must be built in the gNB before the RAP starts. Since the length of signature L is defined in the SIB 1, the time required to transmit a signature varies from 23, 53, to 83 as given in Table 2. Based on Section 3.4, a list of D_t signatures will be decoded by gNB. With this list and the format in Figures 13, 14, and 15, gNB generates the SR and broadcasts it to MTCDs. An MTCD obtains its uplink resource allocation if its Cell Sequence appears in the received SR. Due to the uniqueness of Cell Sequence, it is impossible for more than one MTCD to send the Scheduled Transmission on the same uplink radio resource. In other words, in the proposed design, there is no Scheduled Transmission collision problem. However, as mentioned in Section 3.5, the signature decoding may result in the false positive problem. In the proposed design, the impact of the false positive problem comes from the waste of allocating uplink radio resources to the MTCDs whose signatures are falsely decoded by the gNB. After receiving the Contention Resolution from the gNB, the procedures of the proposed 4-step Signature RA type are completed and the MTCD proceeds to send small data accordingly.

When $C = 1,000$ and $K = 4$, the average number of false positives of the proposed 4-step Signature RA type with respect to different values of L is shown in Figure 16. It can be seen from Figure 16 that, for any value of C_{active} , the number of false positives is decreased as the value of

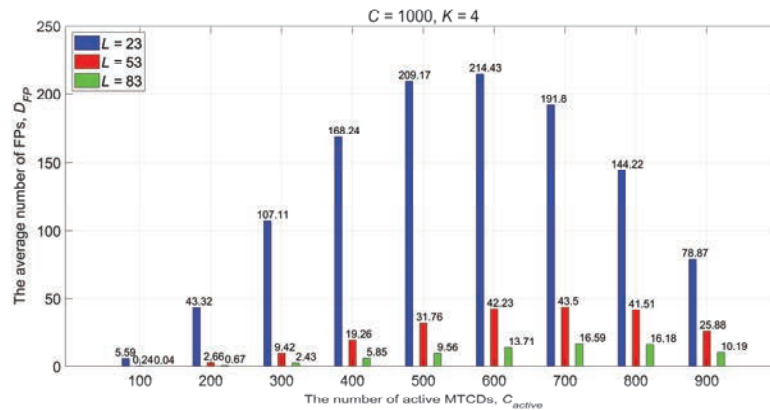


Figure 16 Average number of false positives with different L in 4-step Signature RA type.

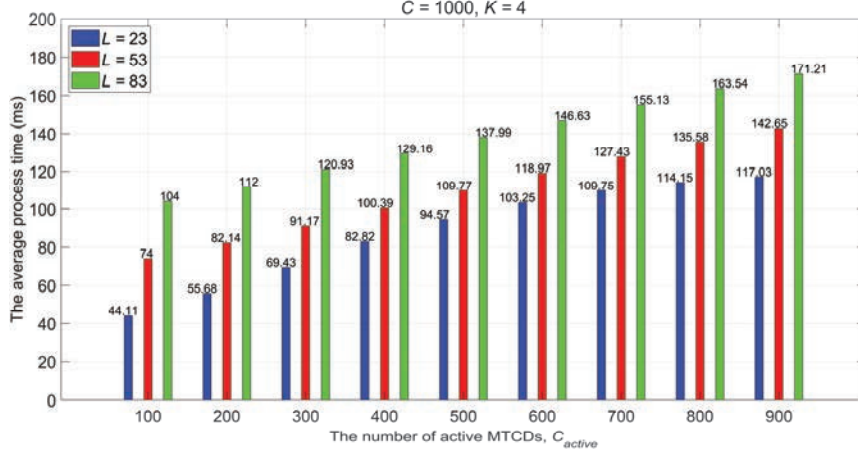


Figure 17 Average process time with different L in 4-step Signature RA type.

L is increased. This is mainly because the differences between signatures are increased as the value of L is increased. Consequently, gNB can be much easier to identify MTCDs. In addition, as the increase of C_{active} , the number of false positives is increased accordingly. The reason for this is the number of received signatures increases when C_{active} is increased. Hence, the number of preambles in the received signature \mathbf{Y} in (8) is increased. As a result, more number of signatures of inactive MTCDs satisfy (9) and are falsely decoded. However, due to the number of inactive MTCDs decreases as C_{active} approaches C , the number of false positives decreases.

Figure 17 shows the average process time to complete the proposed 4-step Signature RA type with respect to different values of L . Since the number of RAOs for a signature increases as L is increased, the time required to send a signature is also increased. Therefore, the average process time is increased as L is increased. Besides, due to the value of D_t in (10) increases as C_{active} is increased, the number of SRs increases and the time for gNB to send and for MTCD to receive the SRs are increased. As a consequence, the average process time in Figure 17 also increases as C_{active} is increased.

When $C = 1,000$ and $L = 53$, Figures 18 and 19 are the average number of false positives and the average process time of the proposed 4-step Signature RA type for different values of K . It can be seen in Figure 18, when C_{active} is not so many, say 100 to 300, due to fewer number of signatures consists of the received signature \mathbf{Y} in the gNB, higher value of K reduces the similarity among signatures. Thus, the number of false positives is also

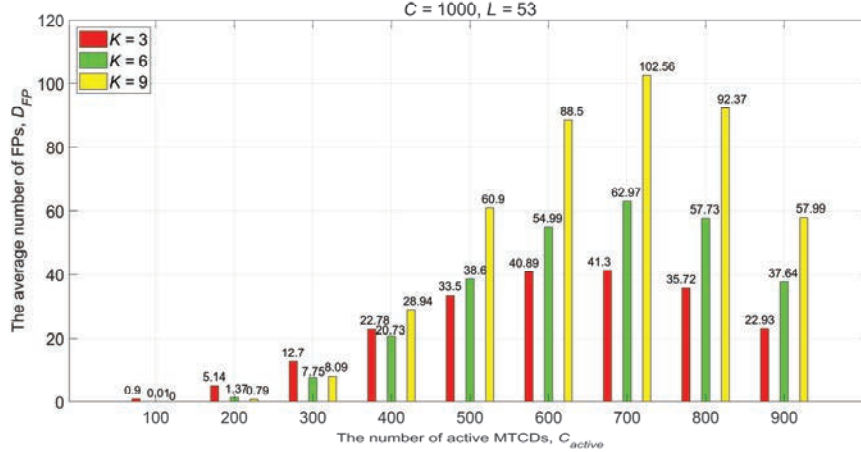


Figure 18 Average number of false positives with different K in 4-step Signature RA type.

reduced. However, as C_{active} is larger than 400, a larger number of signatures consists of the received signature \mathbf{Y} in the gNB. In addition, what even worse is the number of preambles in the received signature \mathbf{Y} increases if K is increased. This results in more signatures being falsely decoded. Hence, it can be found in Figure 18 that a higher value of K is with the larger average number of false positives when C_{active} is larger than 400. When C_{active} is 400, smaller K , e.g., $K = 3$, results in fewer preambles in the received signature \mathbf{Y} . On the contrary, larger K , e.g., $K = 9$, results in more number of preambles in the received signature \mathbf{Y} . However, unfortunately, both cases result in an increase in the number of false positives. Hence, when C_{active} is 400, the least average number of false positives is observed when $K = 6$.

Figure 19 demonstrates the average process time of the proposed 4-step Signature RA type is basically proportionally to the value of C_{active} . Since the value of K affects the number of false positives, therefore, it affects the time to send and receive the SR. However, Figure 19 shows the affection to the average process time is limited.

Finally, the average number of preamble attempts and the average process time for the 5G NR 4-step RA type and the proposed 4-step Signature RA type are shown in Figures 20 and 21, respectively. Here, the parameter values of the proposed 4-step Signature RA type are $C = 1,000$, $L = 23$, and $K = 4$. In Figure 20, due to the collisions resulting from different active MTCs selecting the same preamble and sending it to the gNB in the same RAO, the average number of preamble attempts for the C_{active} active MTCs

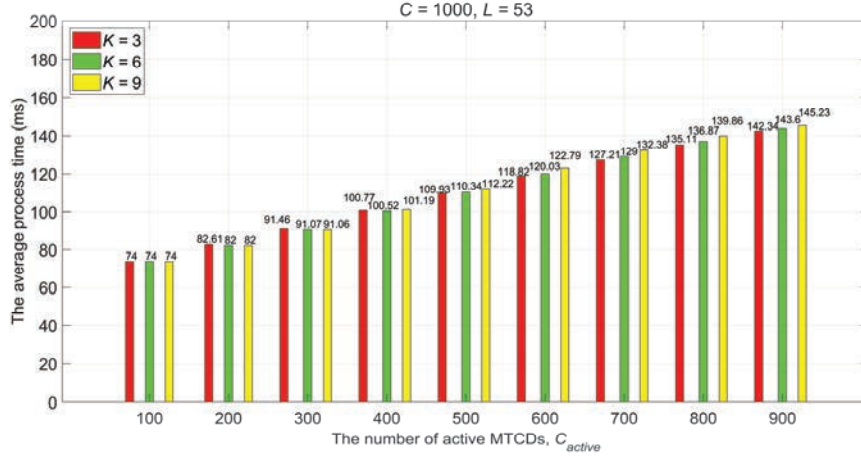


Figure 19 Average process time with different K in 4-step Signature RA type.

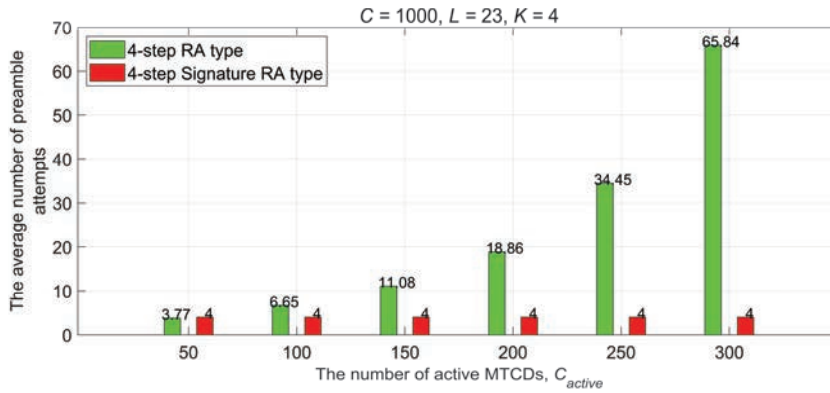


Figure 20 Average number of preamble attempts.

to complete the RAP of the 5G NR 4-step RA type increases dramatically as C_{active} is increased. However, when L and K are fixed, the average number of preamble attempts in the proposed 4-step Signature RA type is independent of C_{active} . Hence, the average number of preamble attempts remains the same value as C_{active} is increased.

As the discussions above, the average number of preamble attempts to complete the RAP of the 5G NR 4-step RA type increases greatly as C_{active} is increased. Hence, the average process time to complete the RAP of the 5G NR 4-step RA type shown in Figure 21 also greatly increases as C_{active} is

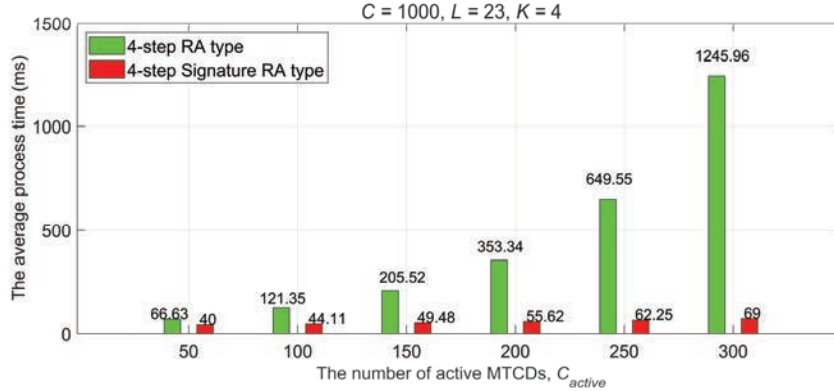


Figure 21 Average process time.

increased. However, since there is no uplink collision in the proposed 4-step Signature RA type, the increase of C_{active} mainly increases the time to send and receive the SRs, which results in a minor increase in the average process time in Figure 21. The results shown in Figures 20 and 21 confirm that the proposed 4-step Signature RA type performs much better than the existing 5G NR 4-step RA type in the mMTC application scenario.

5 Conclusion

This paper proposes the design of the modified CBRA with 4-step RA type and 4-step Signature RA type for the mMTC application scenarios. The modified CBRA with 4-step RA type is used for the MTCD to obtain the information required to generate the signature. With the signature, the 4-step Signature RA type is used for MTCDs to set up the RRC connection to the gNB. Performances of the proposed design are verified by simulations coded in MATLAB. In the simulations, different parameter values are used to evaluate the effects on the average number of false positives and average process time. In addition, this paper also compares the average number of false positives and average process time between the 5G NR 4-step RA type and the proposed 4-step Signature RA type. Simulation results show that the proposed 4-step Signature RA type outperforms the 5G NR 4-step RA type from the perspectives of the average number of preamble attempts and the average process time.

References

- [1] M. Series, 'Minimum requirements related to technical performance for IMT-2020 radio interface (s).' ITU, Geneva, Switzerland, Rep. M.2410-0, 2017.
- [2] 3GPP TS 22.368 V17.0.0, 'Service requirements for Machine-Type Communications,' Mar. 2022.
- [3] 3GPP TS 38.300 V17.3.0, '5G; NR; NR and NG-RAN Overall description; Stage-2,' Dec. 2022.
- [4] C. Tseng, L. Wang, F. Kuo, and H. Wang, 'The Design of Low-Latency Random Access Procedure for 5G,' 2020 IEEE International Conference on Communications (ICC). IEEE, 2020.
- [5] C. Tseng, H. Wang, J. Chang, L. Wang, and F. Kuo, 'Design of Two-Step Random Access Procedure for URLLC Applications,' *Wireless Personal Communications*, vol. 121, no. 2, pp. 1187–1219, September 2021.
- [6] Sassan. Ahmadi, *5G NR: Architecture, technology, implementation, and operation of 3GPP new radio standards*. Academic Press, 2019. pp. 627–628.
- [7] 3GPP TS 37.868 V11.0.0, 'Study on RAN improvements for Machine-type Communications,' Sep. 2011.
- [8] C. Wan and J. Sun, 'Access Class Barring Parameter Adaptation Based on Load Estimation Model for mMTC in LTE-A,' 2019 International Conference on Communications, Information System and Computer Engineering (CISCE), Haikou, China, 2019, pp. 512–515.
- [9] Nuno K. Pratas, et al., 'Massive machine-type communication (mMTC) access with integrated authentication.' 2017 IEEE International Conference on Communications (ICC). IEEE, 2017.
- [10] Nuno K. Pratas, et. al., 'Random access for machine-type communication based on bloom filtering.' 2016 IEEE Global Communications Conference (GLOBECOM). IEEE, 2016.
- [11] 3GPP TS 38.321 V17.3.0, '5G; NR; Medium Access Control (MAC) protocol specification,' Dec. 2022.
- [12] 3GPP TS 38.331 V17.3.0, 'Radio Resource Control (RRC); Protocol specification,' Dec. 2022.

Biographies



Wei-Chieh Wang received the B.S. and M.S. degrees in Department of Electrical Engineering from National Ilan University in 2020. His research interest and expertise are in mobile communications.



Yao-Jen Liang received the Ph.D. degree in Communication Engineering from National Taiwan University, Taiwan, in 2010. He has more than six years experience in industry. From 2010 to 2011, he was a postdoctoral fellow at Institute of Information Science, Academia Sinica, Taiwan. From February 2011 to February 2012, he was a visiting scholar at the School of Electrical and Computer Engineering, Georgia Institute of Technology. He is currently an associate professor with the Department of Electronic Engineering, National Ilan University. His current research interests include MIMO and OFDM systems, statistical signal processing, and molecular communications.



Hwang-Cheng Wang received an M.S. degree in Computer Science and a Ph.D. degree in Electrical Engineering, both from the University of Southern California, Los Angeles, California, USA. He is a professor in the Department of Electronic Engineering, National Ilan University (NIU), Taiwan. He is the director of the Embedded Systems and Mobile Computing Laboratory at NIU. Prior to joining NIU, he was with the Data Communication Institute, Ministry of Transportation and Communications. He has been a visiting scholar at the Next Generation Internet Research Center, Beijing Jiaotong University, Information Science Institute, Academia Sinica, and LNM Institute of Information Technology, India. His research interests and expertise are in mobile communications, embedded systems, internet of things, machine and deep learning, and UAV. He has authored or co-authored journal and conference papers in these areas. He has also served as a technical committee member of international conferences and a reviewer for reputed journals and conferences.



Fang-Chang Kuo received the B.S. degree in E. E. from Tatung University in 1986, and Ph.D. degree in E. E. from National Central University, Taiwan, in

1997. He is currently a professor with the Department of Electronic Engineering, National Ilan University, Taiwan. Since 2014, he was a visiting scholar with the Department of Computer Science, University of Freiburg, Germany for one year. His research interests are in the areas of AIoT, communication networks and wireless communications.



Chih-Cheng Tseng received his B.S. and M.S. degrees from the National Taiwan University of Science and Technology, Taipei, Taiwan, Republic of China, in 1994 and 1997 respectively, all in Electronic Engineering. He received his Ph.D. degree from the Graduate Institute of Communications Engineering, National Taiwan University, Taipei, Taiwan, Republic of China, in 2007. He is currently a full professor with the Department of Electrical Engineering, National Ilan University, Yilan, Taiwan, Republic of China. He was a visiting researcher at the Center for TeleInFrastruktur (CTIF), Aalborg University, Denmark in 2007 summer. He has been actively involved in professional activities, serving as a Sponsorship Co-Chair of IEEE Globecom 2020, TPC Co-Chair of Qshine 2015 and WPMC 2023, co-organizer of NGWiFi workshop in IEEE WCNC 2014, HetCarrierCom workshop in IEEE Globecom 2015, 5G CAT workshop in Qshine 2016, and New Radio Technologies workshop in IEEE PIMRC 2017, general secretariat of WPMC 2012, special session organizer of the GWS 2013 and GWS 2014, and reviewer for SCI journals and international conferences. He is currently serving as the editor of the international journals IET Electronic Letters (SCI) and Journal of Mobile Multimedia. He also served as the guest editor of SCI journals such as International Journal of Sensor Networks, Wireless Personal Communications, and Wireless Communications and Mobile Computing. His research interests include the design and performance evaluation of the next generation mobile communication technologies.

