# Detection Probability of PBCH Demodulation Reference Signal Sequence in the Presence of Jamming

**Shun YONEDA**[†], ***Student Member***, **Mamoru SAWAHASHI**[†], ***Fellow***, ***and*** **Satoshi NAGATA**[††], ***Member***

**SUMMARY** Radio access networks (RANs) based on the New Radio (NR) standard in the 3rd generation partnership project (3GPP) achieve a higher system capacity, higher spectral efficiency, higher peak data rate, and lower latency than that for the Long Term Evolution (LTE) standard. Similar to LTE based RANs, NR based RANs are used for broadcasting emergency and public safety information due to its advantageous features. Because of their important nature, the security of these RANs is vital and assessing the robustness of the physical channels against a jamming signal is necessary. This paper investigates the correct detection probability (CDP) of a demodulation reference signal (DMRS) sequence for the NR physical broadcast channel (PBCH), which a jammer can effectively use to implement a denial of service (DoS) attack on the NR RAN to disrupt the public safety feature in the network. To the best knowledge of the authors, the quantitative effect of the DMRS sequence in the PBCH when affected by a jamming signal has not yet been reported. Computer simulation results show that the impact on the CDP of the PBCH DMRS sequence by a jamming signal is small when the received jamming-to-DMRS power level is lower than approximately 10 dB.

***key words:*** *DMRS sequence, PBCH, jamming, detection probability, denial of service*

## 1. Introduction

The 5G cellular systems based on the New Radio (NR) standard in the 3rd generation partnership project (3GPP) support three major deployment scenarios: enhanced mobile broadband (eMBB), massive machine type communications (mMTC), and ultra-reliable low latency communications (URLLC) [1]. The waveform and numerologies of the 5G NR radio interface are based on those of the Long Term Evolution (LTE) radio interface [2]. The LTE radio interface is employed for broadband emergency information, announcing natural disasters, and other crises in addition to cellular network services [3]. It has also been adopted for mission-critical applications such as public safety. Because of its superior performance to LTE -Advanced [1], the 5G NR radio interface will be used for mission-critical services including public safety in the next decade. Hence, the 5G NR radio access network (RAN) should be secure and robust against deliberate radio frequency (RF) interference and jamming. The vulnerability of the NR physical channels to jamming and RF spoofing was investigated in [4]. Attacks on the radio interface are roughly categorized into denial of service (DoS) and information extraction [3]. Between these, information extraction is almost impossible due to strict authentication, encryption, and integrity in the higher layer. However, jamming attacks are used to disrupt available reliable service or for DoS. For initial access in the NR downlink, the synchronization signal block (SSB) is specified for a set of user equipment (UE) to search a physical-layer cell identity (PCID) of the best cell site that provides the maximum received signal power level. The SSB comprises the primary synchronization signal (PSS), secondary synchronization signal (SSS), and physical broadcast channel (PBCH). Figure 1 shows the flow of the NR downlink initial access using the SSB. A UE first detects the received timing and the sequence of the PSS in the SSB. Because the relative interval between the PSS and SSS is known to a UE, the UE detects the SSS sequence based on the received timing of the PSS. The UE detects the PCID of the best cell among 1,008 candidates from the combination of the PSS and SSS sequences. From the estimated PCID, the UE detects the demodulation reference signal (DMRS) sequence in the PBCH. The PBCH payload is coherently demodulated based on the channel response at each subcarrier position using the DMRS in a frequency-selective fading channel. The PBCH carries the master information block (MIB), which contains control information essential for initial access in a cell including the downlink system bandwidth, a part of the SSB index, and other control information. Therefore, a UE cannot access the desired cell site as long as the MIB bits in the PBCH are not demodulated and decoded correctly. Hence, one of the most effective NR physical channels for a jammer to implement a DoS is the PBCH. In the resource elements (REs) in the PBCH, the DMRS is multiplexed into one RE among every four REs where the payload of the PBCH is multiplexed. Therefore, it is more effective for a jammer to transmit a jamming signal to the DMRS that is multiplexed sparsely in the PBCH than directly to the payload of the PBCH. When the detection of the DMRS sequence fails, the decoding of the PBCH payload will fail. To the best knowledge of the authors, however, the quantitative effect of the DMRS sequence in the PBCH when affected by a jamming signal has not yet been reported.

This paper investigates the correct detection prob-

[†]The authors are with Tokyo City University, Setagaya-ku, Tokyo, 158-8557 Japan.
[††]The author is with NTT DOCOMO INC., Kanagawa-ken, 239-0847 Japan.

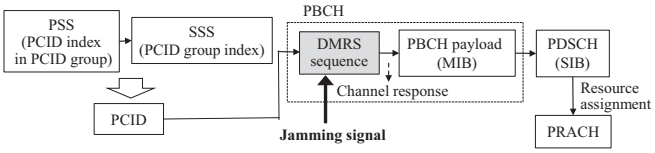


**Fig. 1** Initial access procedure for NR radio interface.

ability (CDP) of the DMRS sequence in the PBCH for the NR radio interface considering the intended jamming signal. In this paper, we investigate the effect of the jamming signal on the CDP of the PBCH DMRS sequence using the ratio of the received jamming signal power to the DMRS power, $J/S$, as a parameter. The rest of the paper is organized as follows. In Section 2, we describe the SSB structure and the PBCH DMRS sequence. Section 3 describes the PBCH DMRS sequence detection method. Section 4 presents computer simulation results, followed by our concluding statements in Section 5.

## 2. PBCH DMRS in SSB

### 2.1 SSB Structure

Figure 2 shows the SSB structure [2]. The SSB comprises four orthogonal frequency division multiplexed (OFDM) symbols that contain the PSS, SSS, and PBCH associated with the DMRS. The PSS and SSS are multiplexed in OFDM symbol indices #0 and #2 within the SSB, respectively. Three PSS sequences are specified that are M-sequences with different cyclic shifts. The PSS sequence represents a PCID index within the same PCID group. Meanwhile, 336 SSS sequences are specified based on the Gold sequence. The SSS sequence represents the PCID group index. In the frequency domain, the total number of subcarriers in the SSB is 240, *i.e.*, 20 physical resource blocks. The PSS and SSS are multiplexed in the central part with 127 subcarriers in the SSB. We let $k$ be the subcarrier index within the SSB with a 240-subcarrier bandwidth ($0 \le k \le 239$). The PSS and SSS are multiplexed in the 127 subcarriers from the subcarrier index of $k$ = 56 to $k$ = 182. The PBCH associated with the DMRS is multiplexed in the 240 subcarriers at OFDM symbol indices #1 and #3. Moreover, the PBCH associated with the DMRS is multiplexed from subcarrier index $k$ = 0 to 47 and from $k$ = 192 to 239 at OFDM symbol index #2. Because the DMRS sequence length is 144, the DMRS is multiplexed every four REs along subcarriers from OFDM symbol #1 in the PBCH. A different RE that is shifted by one RE is assigned to the DMRS according to the integer value of $\nu = N_{ID}^{cell}$ mod 4 ($\nu$ = 0, 1, 2, and 3). At OFDM symbol index #1, the DMRS with the index of $0 \le u < 60$ is multiplexed at subcarrier $k$ in the region of $0 \le k < 240$ where $k$ is represented as $k = \nu + 4u$. Similarly, at OFDM symbol #2, the DMRS with the index of $60 \le u < 72$ and that of $72 \le u < 84$ are multiplexed at subcarrier index $k = \nu + 4(u - 60)$ and $k = 192 + \nu + 4(u - 60)$, respectively. At OFDM symbol index #3, the DMRS with the index of $84 \le u < 144$ is multiplexed at subcarrier $k$ in the region of $0 \le k < 240$ with $k = \nu + 4(u - 84)$.

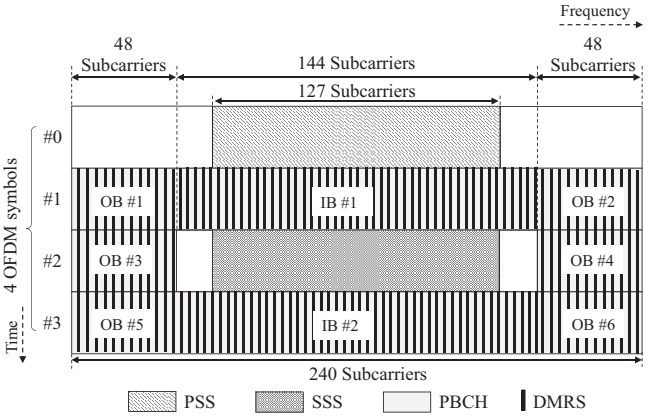


**Fig. 2** PBCH DMRS multiplexing in SSB.

### 2.2 PBCH DMRS Sequence

The DMRS sequence in the PBCH is generated using a Gold sequence as shown below [2].

$$r(m) = \frac{1}{\sqrt{2}}(1 - 2 \cdot c(2m)) + j\frac{1}{\sqrt{2}}(1 - 2 \cdot c(2m+1)), \quad (1)$$

where $c(n)$ is a Gold sequence that is specified as

$$c(n) = (x_1(n + N_c) + x_2(n + N_c)) \mod 2. \quad (2)$$

In (2), $N_c = 1600$ and the generator polynomials of the two M-sequences are given as

$$\begin{cases} x_1(i+31) = [x_1(i+3) + x_1(i)] \mod 2 \\ x_2(i+31) = [x_2(i+3) + x_2(i+2) + x_2(i+1) \\ \qquad\qquad +x_2(i)] \mod 2. \end{cases} \quad (3)$$

For frequency spectra above 3 GHz to 6 GHz, the number of SSBs in the 20-ms SSB multiplexing interval is $N_{SSB} = 8$. The DMRS sequence is initialized using a combination of the PCID and the three least significant bits of the SSB index from 0 to 7. The initial value of $x_1(n)$ is given as $x_1(0) = 1$ and $x_1(n) = 0$, $n = 1, 2, , ..., 30$. The initial value of $x_2(n)$ is given by $c_{init} = \sum_{i=0}^{30} x_2(i) \cdot 2^i$, which is represented in the equation below.

$$c_{init} = 2^{11}(\bar{i}_{SSB} + 1)(\lfloor N_{ID}^{cell}/4 \rfloor + 1) + 2^6(\bar{i}_{SSB} + 1) + (N_{ID}^{cell} \mod 4) \quad (4)$$

In (4), $\bar{i}_{SSB}$ indicates the SSB index with values from 0 to 7. From (4), we see that the detection probability of the DMRS sequence is subject to that of the PCID, $N_{ID}^{cell}$.

## 3. PBCH DMRS Sequence Detection Method

At a UE receiver, we employ two-antenna receiver diversity ($h$ = 0,1). In this paper, we assume that a legitimate UE detects the PSS and SSS of the target cell site

ideally. Hence, we assume the ideal estimation of the PCID in (4). We also assume that a jammer sniffs and detects the PSS and SSS of the target cell site ideally and transmits a jamming signal targeting the PBCH DMRS resource to implement a DoS attack on a legitimate UE. As shown in Fig. 2, the DMRSs are divided into two parts according to the bandwidth in which the DMRSs are multiplexed: those that are multiplexed in the same bandwidth as the PSS and SSS, and those that are multiplexed outside the bandwidth of the PSS and SSS. We should estimate the channel response of the REs for the central parts of the DMRS in OFDM symbols #1 and #3 using the PSS and SSS in the same bandwidth in a multipath fading channel. Hence, we employ the individual computation processes for a partial PBCH DMRS sequence [5]. The DMRS index is represented as $14 \leq u < 46$ and $98 \leq u < 130$ for the DMRSs that are multiplexed in the same bandwidth as the PSS and SSS at OFDM symbols #1 and #3, respectively (we denote the two blocks of the DMRSs at OFDM symbols #1 and #3 as IB#1 and IB#2, respectively). For these DMRSs, the correlation of the DMRS is computed after the channel response of the received DMRS is compensated. We estimate the channel response of the REs where the DMRSs are multiplexed using the PSS and SSS. For the DMRSs of $14 \leq u < 46$ at OFDM symbol #1, the channel response at subcarrier position $k$ is computed using the detected PSS and SSS with the relation of $k = \nu + 4u$ with $\nu = N_{ID}^{cell}$ mod 4. The channel response using the PSS and SSS is given as $\bar{H}_{IB\#1}^{(h)}(k) = \{\hat{R}_{PSS}^{(h)}(k) \times d_{PSS}(k)^* + \hat{R}_{SSS}^{(h)}(k) \times d_{SSS}(k)^*\}/2$. Here, $\hat{R}_{PSS/SSS}^{(h)}(k)$ denotes a channel response estimate at subcarrier $k$ using the PSS or SSS, and $*$ denotes complex conjugate. For the DMRS of $98 \leq u < 130$ in OFDM symbol #3, the channel response at subcarrier position $k$ is computed using only the SSS as $\bar{H}_{IB\#2}^{(h)}(k) = \hat{R}_{SSS}^{(h)}(k) \times d_{SSS}(k)^*$ using the relation of $k = \nu + 4(u - 84)$. The channel response at subcarrier position $k$ is further averaged coherently in the frequency domain to reduce the additive white Gaussian noise as $\tilde{H}_{IB\#1/\#2}^{(h)}(k) = \frac{1}{2N_{CE}^{DMRS}+1} \sum_{\eta=-N_{CE}^{DMRS}}^{N_{CE}^{DMRS}} \bar{H}_{IB\#1/\#2}^{(h)}(k+\eta)$, where $N_{CE}^{DMRS}$ denotes the number of subcarriers on one side for averaging the channel response. Hence, by using the relation of $u = \bar{u} + (k - \nu)/4$ ($\bar{u} = 0$, 60, 84 for OFDM symbol index #1, #2, and #3, respectively), the partial DMRS correlation is computed for the DMRS indexes of $14 \leq u < 46$ and $98 \leq u < 130$ as

$$\bar{R}_{IB\#1/\#2}^{(h)} = \frac{1}{32} \sum_{u=u_0}^{u_0+31} R^{(h)}(u) \times \tilde{H}_{IB\#1/\#2}^{(h)}(u)^* \times C_{DMRS}(u)^*. \quad (5)$$

Here, $C_{DMRS}(u)$ denotes the DMRS sequence, and $u_0$ denotes the starting DMRS sequence index for computing the partial DMRS sequence that is given as $u_0 = 4u$ and $u_0 = 98+4u$ for DMRS block IB#1 at OFDM symbol #1 and DMRS block IB#2 at OFDM symbol #3, respectively.

We compute the correlation of the partial DMRS sequence that is multiplexed in the bandwidth outside the PSS and SSS without channel estimation. As shown in Fig. 2, we divide the partial DMRS sequence that is multiplexed in the subcarriers outside of the PSS or SSS into six DMRS blocks (we denote the six DMRS blocks as OB#1 - #6): DMRS sequence index of $0 \leq u \leq 13$ (subcarrier index of $0 \leq k \leq 55$) for block OB#1; $46 \leq u \leq 59$ (subcarrier index of $184 \leq k \leq 239$) for block OB#2; $60 \leq u \leq 71$ (subcarrier index of $0 \leq k \leq 47$) for block OB#3; $72 \leq u \leq 83$ (subcarrier index of $192 \leq k \leq 239$) for block OB#4; $84 \leq u \leq 97$ (subcarrier index of $0 \leq k \leq 55$) for block OB#5; and $130 \leq u \leq 143$ (subcarrier index of $184 \leq k \leq 239$) for block OB#6. Each of the six DMRS blocks is further divided into sub-blocks in which the correlation of the partial DMRS sequences is computed coherently. The computed correlation of each sub-block is averaged between the sub-blocks in each block in squared form. The number of sub-blocks is set to $N_{sb} = 1$ [5]. The resultant correlation of the partial DMRS sequence is computed as

$$\bar{R}_{OB\#\beta}^{(h)} = \frac{1}{N_{sb}} \sum_{b=0}^{N_{sb}-1} \left| \frac{1}{M} \sum_{u=u_0}^{(M+u_0)} R^{(h)}(u+bM) \times C_{DMRS}(u+bM)^* \right|^2. \quad (6)$$

Here, $M = N_{OB\#\beta}^{DMRS}/N_{sb}$ and $\beta$ represent a DMRS block index in the bandwidth outside of the PSS and SSS ($\beta \in \{1, ..., 6\}$). Term $N_{OB\#\beta}^{DMRS}$ denotes the number of chips for the partial DMRS sequence of DMRS block $OB\#\beta$; $N_{OB\#\beta}^{DMRS} = 14$ for $OB\beta = 1$, 2, 5, and 6, and 12 for $OB\beta = 3$ and 4. The $u_0$ is 0, 46, 60, 72, 84, and 130 for DMRS blocks OB#1, OB#2, OB#3, OB#4, OB#5, and OB#6, respectively. We detect the PBCH DMRS sequence that provides the maximum correlation power as shown in the equation below.

$$\hat{i}_{SSB} = \arg\max_{\bar{i}_{SSB}} \sum_{h=0}^{1} \left\{ \left( \frac{\sum_{\alpha=1}^{2} \bar{R}_{IB\#\alpha}^{(h)}}{2} \right)^2 + \frac{1}{6} \sum_{\beta=1}^{6} \bar{R}_{OB\#\beta}^{(h)} \right\} \quad (7)$$

In (7), $\alpha$ is a DMRS block index in the same bandwidth as the PSS and SSS ($\alpha \in \{1, 2\}$).

## 4. Computer Simulation Results

We investigate the CDP of the PBCH DMRS sequence of the legitimate UE considering jamming in multipath Rayleigh fading channels. In the simulation, we assume the carrier frequency of $f_c = 4$ GHz and the subcarrier spacing of 30 kHz. We assume the 3GPP Tapped Delay

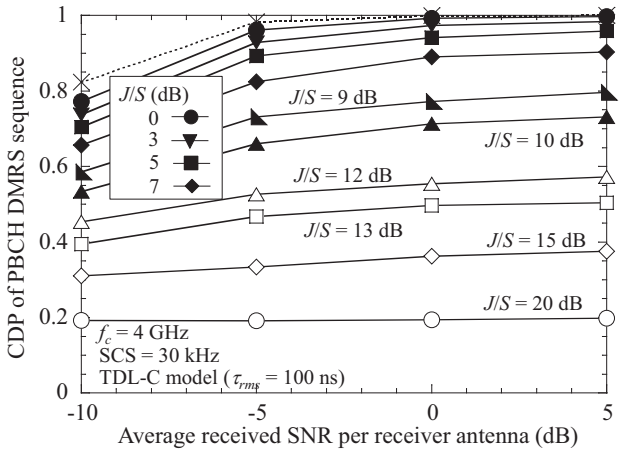


**Fig. 3** CDP of PBCH DMRS sequence for $J/S$ without CFO.

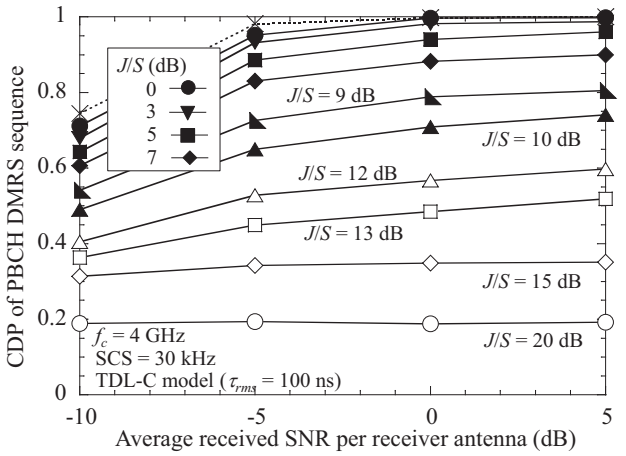


**Fig. 4** CDP of PBCH DMRS sequence for $J/S$ with CFO.

Line (TDL)-C channel model with the root mean square delay spread of $\tau_{rms} = 100$ ns [6]. Because we assume the moving speed of a UE of 3 km/h, the maximum Doppler frequency becomes $f_D = 11.1$ Hz.

Figure 3 shows the CDP of the PBCH DMRS sequence as a function of the average received signal-to-noise ratio (SNR) per receiver antenna with $J/S$ as a parameter. We do not consider the carrier frequency offset (CFO) in Fig. 3. We plot the CDP without the jamming signal as a dotted line. The figure shows that according to the increase in the $J/S$ value, the CDP of the PBCH DMRS sequence is degraded due to the increasing jamming interference. When $J/S = 5$ dB and 10 dB, the CDP of the PBCH DMRS sequence is degraded by approximately 4% and 27% compared to that without the jamming signal. Hence, we see that the PBCH DMRS sequence is tolerant to the jamming signal with a received power level of lower than approximately $J/S = 10$ dB. However, when the $J/S$ increases higher than approximately 13 dB, the CDP of the PBCH DMRS sequence becomes less than 50%.

Figure 4 shows the CDP of the PBCH DMRS sequence with $J/S$ as a parameter taking into account the CFO due to the high frequency stability of a UE local oscillator. In the simulation, we set the frequency stability of a UE local oscillator to $\varepsilon = 3$ ppm, which corresponds to the maximum CFO of 12 kHz. We used the fractional frequency offset (FFO) estimation method based on the partial correlation of the PSS and the joint estimation of the integer frequency offset (IFO) associated with the SSS sequence [7]. Then, we added the residual CFO to the PBCH after compensating the estimated FFO and IFO. Figure 4 shows that the CDP of the DMRS sequence with the residual CFO is slightly degraded compared to that without the CFO in Fig. 3. However, we find the same tendency for the effect of $J/S$ as that in Fig. 3. We see that the CDP of the PBCH DMRS sequence becomes less than 50% when $J/S$ increases higher than 13 dB.

We briefly describe mitigation techniques for the intended jamming. PSS spoofing can be mitigated by creating a timer for receiving the SSS. If the timer expires, a UE should blacklist the PSS and choose the cell with the second highest power within the same frequency band [3]. Another method is to have the UE search for the PSS and SSS of the SSB located on a different synchronization raster by changing the frequency so that it detects the PBCH DMRS sequence and decodes the PBCH payload correctly.

## 5. Conclusion

In this paper, we investigated the CDP of the PBCH DMRS sequence with which a jammer can effectively cause a DoS in NR RANs. Computer simulation results showed that the PBCH DMRS sequence is robust against a jamming signal as long as the received jamming power level is lower than approximately $J/S = 10$ dB. Meanwhile, when the $J/S$ value exceeds approximately 13 dB, the CDP of the PBCH DMRS sequence becomes less than 50%.

### References

[1] 3GPP TR 38.912, “Study on New Radio (NR) access technology (Release 15)," V15.0.0, June 2018.
[2] 3GPP TS 38.211, “NR; Physical channels and modulation (Release 15),” V1.2.0, Nov. 2017.
[3] M. Lichtman, R. P. Jover, M. Labib, R. Rao, V. Marojevic, and J. H. Reed, “LTE/LTE-A jamming, spoofing, and sniffing: Threat assessment and mitigation,” IEEE Commun. Mag., vol. 54, no. 4, pp. 54 - 61, April 2016.
[4] M. Lichtman, *et al.*, “5G NR jamming, spoofing, and sniffing: Threat assessment and mitigation,” Proc. IEEE ICC2018 Workshops, March 2018.
[5] K. Ota, D. Inoue, M. Sawahashi, and S. Nagata, “Radio frame timing detection method using demodulation reference signals based on PCID detection for NR initial access,” IEICE Trans. on Commun., vol. E105-B, no. 6, pp. 775 - 787, June 2022.
[6] 3GPP TR 38.901, “Study on channel model for frequencies from 0.5 to 100 GHz,” V14.3.0, Dec. 2017.
[7] D. Inoue, K. Ota, M. Sawahashi, and S. Nagata, “Physical cell ID detection using joint estimation of frequency offset and SSS sequence for NR initial access,” IEICE Trans. on Commun., vol. E104-B, no. 9, pp. 1120 - 1128, Sept. 2021.