



Wireless Architect Group

wirelessarchitectgroup.com

Demystifying networks for investigators.

WHITE PAPER · CASE STUDY 002

Demystifying TA Short Throws

Why a distant phone can produce a short timing advance record, explained from the 3GPP standards

Author	Reggie Collette, Founder & Principal Architect	Document no.	WAG402-CS002-WP
Audience	Investigators, analysts, and attorneys who work with operator records	Version	rev 0.4
Technologies	4G LTE · 5G NR	Date	September 2026
Companion	Recorded case study WAG-402 CS002	Contact	reggie@wirelessarchitectgroup.com

“Investigators shouldn’t need a PhD in engineering to rely on network data relevant to their investigations. Our mission is to bridge that gap.”

Notices

Copyright, disclaimer of views, references and sources

COPYRIGHT

© 2026 RMC Holdings LLC, d/b/a Wireless Architect Group. All rights reserved. All content herein — text, graphics, diagrams, methodologies and explanatory material — is the exclusive intellectual property of RMC Holdings LLC, protected under U.S. and international copyright law.

This white paper may be shared in its **complete, unmodified form**, including this notice, for non-commercial educational purposes. Branding, logos, hyperlinks, author attribution and copyright notices may not be removed, altered or obscured. Excerpting, adapting, re-teaching, republishing or any commercial use requires the **prior written permission of the author**.

DISCLAIMER OF VIEWS

The views, thoughts, and opinions expressed in this paper are solely the author's own. They are presented in the author's individual capacity and do not represent the positions, policies, or opinions of any past, present, or future employer, client, agency, or entity to which the author has provided consulting or professional services. Nothing herein should be construed as an official statement or endorsement on behalf of any such organization.

NOT LEGAL ADVICE

The author is not an attorney, and nothing in this paper is legal advice. For legal questions, including how any of this material applies to a particular case, consult your own legal counsel.

REFERENCES AND SOURCES

To the fullest extent possible, all concepts, terminology, and technical explanations are drawn from open, publicly available sources, including 3GPP specifications, published industry standards, and other open-source references (see References). Examples, figures, and scenarios are illustrative only. They are not intended to represent how any specific vendor, carrier, or operator designs, configures, or operates its network.

ABOUT THIS PAPER

This white paper is the written companion to Wireless Architect Group's recorded case study **WAG-402 CS002, "Demystifying TA Short Throws."** It covers the same material in more depth, with the tables, worked examples, and references gathered in one place for later use.

FREE ACCESS - TAKE THE WAG-402 COURSE AT NO COST

Want to see this material taught?

The WAG-402 course, which includes the recorded case study that accompanies this paper, is available free of charge. Registration and enrollment are required.

How to get free access:

1. Go to the course page using the link below.
2. Register for an account and enroll in WAG-402.
3. Select the Free Access option. There is no need to purchase the full course series.

► Start the free WAG-402 course: wirelessarchitectgroup.com

Online Courses -> WAG402, View Details -> Request to Enroll

- Enrollment requests approved within 24-48 hours
- Once approved, finalize enrollment details by returning to the course link
- Free options available for this course. No payment required.

1. Executive Summary

The short answer to short throws

Recent field research introduced the term “**TA short throws**” [5]: network-recorded timing advance (TA) values far shorter than a phone’s true distance from the cell site, sometimes by tens of kilometers. That groundwork research named the effect, documented real cases, and urged caution with long-range TA. What it left open is why the effect happens, why only some long-range readings are affected, and what an investigator should do about it.

This paper offers a standards-based answer. **Short throws are real, and they are a designed behavior of LTE random access, not a bug.** When a phone tries to access a cell from beyond that cell’s configured range, its access preamble arrives so late that it lands in the arrival window of the next-lower preamble. The base station (eNB) reports the wrong preamble ID and measures a short TA from the start of that wrong window. The phone sees the mismatch, ignores the RAR response, and retries, and may never get service on that cell. The eNB, however, has already measured a short TA.

Table 1. The three findings of this paper

1 A design feature, not a bug	2 Operator data stays trustworthy	3 Confirm it together
A phone beyond the cell’s planned range sends a preamble that arrives outside its Ncs window. The eNB reads it as the next-lower preamble and measures a short TA from that window. The phone ignores the mismatched reply and retries.	The network faithfully records the TA it actually measured, exactly as designed. No export error or data-pipeline fault is needed to explain the short value. The records keep their integrity; the hard part is reading them correctly.	The effect is extremely rare in the field and hard to reproduce on demand. We propose RAR captures and a lab test rig to confirm it, and we invite industry partners to validate the theory and share results openly.

The mechanism follows directly from the 3GPP physical-layer and MAC specifications (TS 36.211 and TS 36.321) and is reproduced in simulation with the open-source srsRAN 4G PRACH detector. 5G NR defines its PRACH cyclic shifts the same way (TS 38.211 §6.3.3.1), so the same behavior applies. The effect has not yet been captured in the field in a way that is reliably reproducible. We have tried, and Section 12 describes how we propose to do it with a call for partners.

THE GOAL

Remove the mystery. Make short-throw TA records understood, usable and reproducible, so investigators know when to account for them and when to rule them out.

2. Background

TA short throws are documented, but their cause is still open

Timing advance is the timing correction the network gives a phone so that its uplink transmissions arrive at the base station aligned with everyone else’s. Because the correction is proportional to the round-trip delay between phone and site, investigators use recorded TA values to estimate a phone’s distance from the site. In LTE, one TA step is 16 Ts, about 0.521 μs, which corresponds to roughly 78 m. 5G NR networks will have TA steps corresponding to increments that vary with the sub-carrier spacing (SCS), as covered in detail in our WAG-301 course.

Table 2. Where the conversation stands

What's been documented	Phones recorded at a fraction of their true distance, in places where long-range connections are possible.
What's still open	Why it happens, why only some long-range readings are affected, and where the value changes.
What this paper adds	The LTE random access procedure, and how cell range settings can produce a short TA.

Explanations under discussion range from network configuration to the processing and export of operator data [5]. Everyone is working from the best information available. This paper adds to it by focusing on one question: **what do the LTE standards say happens when a phone tries to connect from beyond a cell's planned range?**

3. Cell Range Fundamentals

SIB2 tells the phone how, and from how far, it can access the cell

SYSTEM INFORMATION: MIB, SIB1 AND SIB2

When a phone (UE) enters a new cell, one of the first things it does is read the cell's broadcast system information. The **Master Information Block (MIB)**, read on the PBCH after the synchronization signals give the UE the Physical Cell ID, carries the downlink bandwidth, the System Frame Number and the PHICH configuration. **SIB1** carries identity and access information: PLMN ID, Tracking Area Code, Cell ID, the cell selection threshold (q-RxLevMin), barring status and the schedule for the other SIBs. Neither carries any random access settings.

SIB2 carries every setting the UE needs for its first PRACH attempt, including the ones that set cell range. These parameters are defined by 3GPP, they are mandatory, and every LTE network in the world broadcasts them in the same format. That consistency is what makes the analysis in this paper possible.

Table 3. SIB2 random access and cell range parameters (shaded rows set the PRACH timing budget and cell range)

SIB2 parameter	What it controls
prach-ConfigIndex	Preamble format (maximum range) and the subframes where PRACH is allowed
zeroCorrelationZoneConfig	Cyclic shift size (Ncs), which caps the cell radius
rootSequenceIndex	First Zadoff-Chu root sequence used to build the 64 preambles
prach-FreqOffset	First PRB of the 6-PRB PRACH band
highSpeedFlag	Restricted preamble set for fast-moving UEs
numberOfRA-Preambles	Preambles open for contention-based access
preambleInitialReceivedTargetPower	Target received power for the first preamble
powerRampingStep	Power added on each retry
preambleTransMax	Attempts allowed before random access is declared failed
ra-ResponseWindowSize	How long the UE waits for the RAR (Msg2), which carries the TA
mac-ContentionResolutionTimer	How long the UE waits for Msg4 contention resolution

SIB2 parameter	What it controls
timeAlignmentTimerCommon	How long a received TA stays valid

Source: 3GPP TS 36.331 (RRC) and TS 36.211 (PRACH).

“MAXCELLRANGE” IS A VENDOR SETTING, NOT A 3GPP PARAMETER

Most practitioners think of maximum cell range as the farthest distance from which the operator allows a phone to **access** the cell. Note the word access rather than carry service; that distinction matters and is covered in Section 7. That understanding is correct as far as it goes, but it is only half the story.

There is no 3GPP parameter called MaxCellRange. Radio equipment vendors offer it as a planning convenience: the operator enters one intended range, and the vendor’s software maps it to the standardized parameters that support it. The operator cannot set it to any distance they like, because the standard defines the available steps: **16 N_{cs} values and 4 FDD preamble formats**. Whatever the operator enters, the cell range lands on one of those fixed combinations.

Table 4. How the vendor setting maps to 3GPP parameters

Vendor concept	3GPP parameter	Broadcast in
Cyclic shift size (N_{cs})	zeroCorrelationZoneConfig	SIB2
Preamble format	Implied by prach-ConfigIndex	SIB2
Root sequences	rootSequenceIndex	SIB2

LIMIT 1: THE CYCLIC SHIFT (NCS)

SIB2 signals zeroCorrelationZoneConfig as an integer from 0 to 15. TS 36.211 Table 5.7.2-2 converts that integer into a cyclic shift value, N_{cs}. The standard does not state a cell range for each value, but applying the basic time units gives the range each N_{cs} supports:

$$\text{Range} = (\text{Ncs} \times 800/839 \mu\text{s} - \text{delay spread}) \times c \div 2$$

Table 5. Cyclic shift values (N_{cs}) and the maximum cell range each supports

zeroCorrelationZoneConfig	Ncs (unrestricted set)	Ncs (restricted set)	Max range
1	13	18	1.1 km
2	15	22	1.4 km
3	18	26	1.8 km
4	22	32	2.4 km
5	26	38	2.9 km
6	32	46	3.8 km
7	38	55	4.7 km
8	46	68	5.8 km
9	59	82	7.7 km
10	76	100	10.1 km
11	93	128	12.5 km
12	119	158	16.2 km

zeroCorrelationZoneConfig	Ncs (unrestricted set)	Ncs (restricted set)	Max range
13	167	202	23.1 km
14	279	237	39.1 km
15	419	N/A	59.1 km
0	0	15	118.9 km

Unrestricted = normal set; restricted = high-speed set. Ranges assume 5.2 μ s delay spread. Source: 3GPP TS 36.211, Table 5.7.2-2. The shaded row is used in the worked examples in Section 8.

Proprietary vendor documentation may show slightly different ranges, typically by a few tenths of a kilometer. That usually reflects different delay-spread assumptions; values of 4, 5 or 6 μ s are common. At the level that matters for our discussions here, the numbers agree closely.

LIMIT 2: THE PREAMBLE FORMAT'S GUARD TIME

The second limit comes from the preamble format. Each format reserves a guard time at the end of the preamble so that a late-arriving preamble does not spill into the next subframe. The maximum range the format supports is the guard time multiplied by $c \div 2$.

Table 6. PRACH preamble formats (FDD)

Format	Length	Cyclic prefix	Sequence	Guard time	Max range
0	1 ms	103.1 μ s	800 μ s	96.9 μ s	14.5 km
1	2 ms	684.4 μ s	800 μ s	515.6 μ s	77.3 km
2	2 ms	203.1 μ s	1,600 μ s	196.9 μ s	29.5 km
3	3 ms	684.4 μ s	1,600 μ s	715.6 μ s	107.3 km

1 Ts $\approx$ 32.6 ns. Max range = guard time $\times c \div 2$. Format 4 (TDD only) omitted. Source: 3GPP TS 36.211, Table 5.7.1-1.

SIB2 does not name the preamble format. It broadcasts prach-ConfigIndex (0 to 63), and TS 36.211 Table 5.7.1-2 maps each index to a format and a set of PRACH opportunities. For FDD the mapping is simple: **indices 0–15 use format 0, 16–31 format 1, 32–47 format 2 and 48–63 format 3**. The full table is in Appendix A.

THE CELL RANGE IS THE LOWER OF THE TWO LIMITS

With both SIB2 values in hand, the effective cell range is the lower of the Ncs range and the preamble format range. In the author's 20+ years of experience building and managing live networks, the binding limit has always been the cyclic shift, not the preamble format. A format-limited cell is possible in theory, so both should always be checked.

The practical takeaway is that **cell range is not a mystery value, and no one has to guess it**. It is constrained to the standard tables, and it can be determined directly by capturing SIB2 at the site. That capture does not require expensive equipment. Drive-test setup for collecting TA measurements is covered in Wireless Architect Group's case study WAG-401 CS001. In that case study, we discuss drive-test gear setup and considerations for collecting high-quality TA data to perform a TA error analysis.

CHECK THE CELL RANGE YOURSELF

1. **Capture SIB2** at the site.
2. **Read two fields:** zeroCorrelationZoneConfig and prach-ConfigIndex.
3. **Look up the range** in the Ncs table (Table 5) and the format table (Table 6), and take the lower value.

4. How Preambles Are Built

Each preamble owns an Ncs-wide arrival window

To start random access, the UE sends one PRACH preamble, called **Msg1**, picked at random from the 64 preambles the cell offers. SIB2 defines that set through two values: rootSequenceIndex (the first Zadoff-Chu root) and zeroCorrelationZoneConfig (Ncs).

Each preamble is an 839-sample **Zadoff-Chu (ZC) root sequence**, cyclically shifted by a multiple of Ncs. Its index, 0 to 63, is the **Random Access Preamble ID (RAPID)** that the eNB echoes back in Msg2. Cyclic shifts of one root do not correlate with each other, so the eNB can tell them apart even when several UEs transmit in the same PRACH slot.

The number of preambles one root can produce is $\lfloor 839 \div \text{Ncs} \rfloor$. With $\text{Ncs} = 119$, one root yields 7 preambles, so the cell needs $\lceil 64 \div 7 \rceil = 10$ roots to reach 64. The UE steps through consecutive root indices, starting at the SIB2 value, until it has all 64.

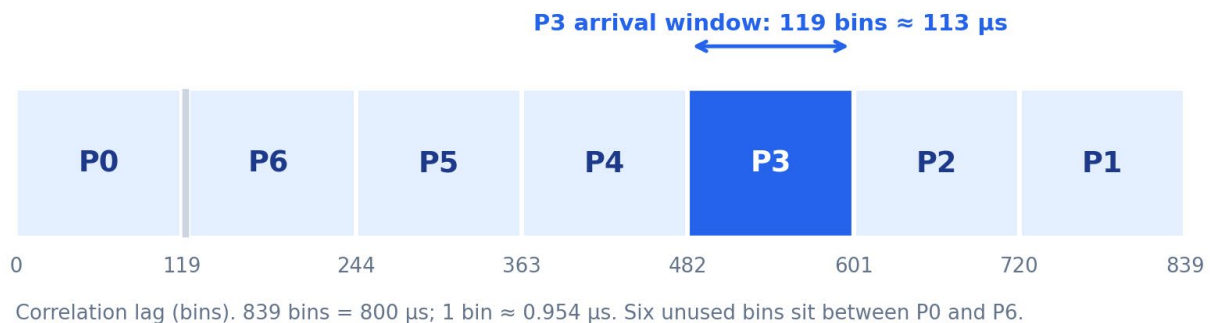


Figure 1. One ZC root sequence with $\text{Ncs} = 119$. In lag order, P0 comes first, then P6 down to P1. Each Ncs block is also that preamble's arrival window.

The key idea is that **each Ncs block is also that preamble's arrival window**. With $\text{Ncs} = 119$, the eNB accepts preamble 3 with up to 119 bins (about 113 μ s) of delay. Distance delays the received preamble, moving it later, to the right, within its window. Past Ncs, the delayed P3 falls into P2's window and looks like the preamble below it. **Ncs therefore sets the maximum cell range.**

5. Where the Spike Lands

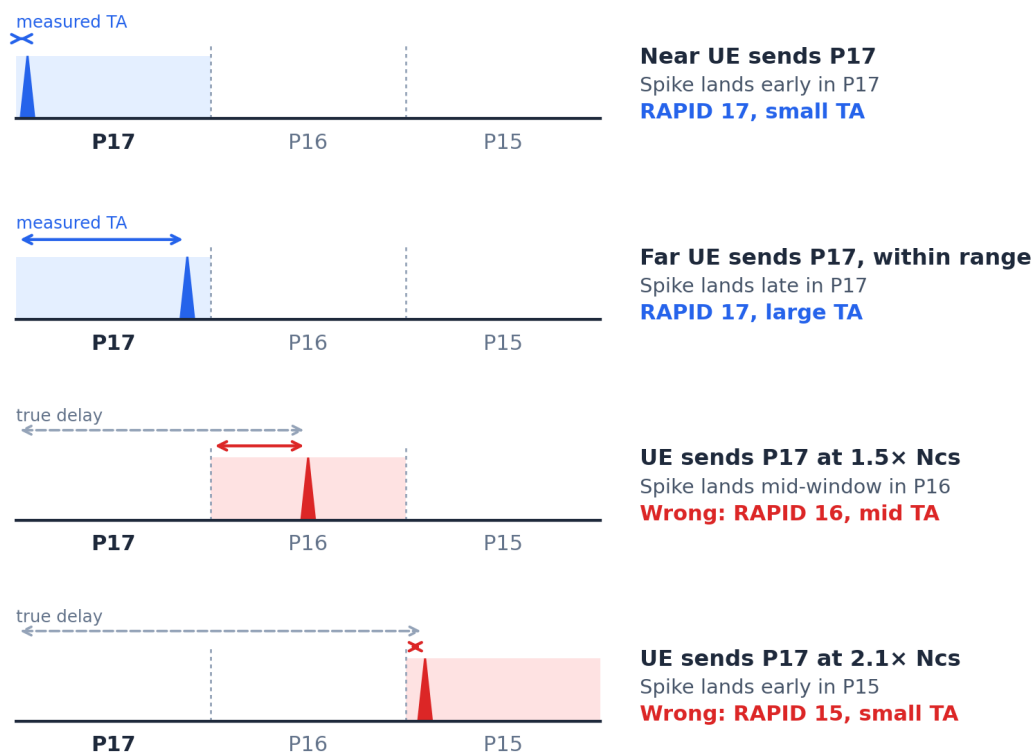
The window identifies the preamble; the position inside it is the delay

The eNB does not know in advance which preamble a UE sent. It correlates the received PRACH signal against its known root sequences, and each preamble produces one **correlation spike**. Two things are read from that spike:

- **Which window it lands in** identifies the preamble, which the eNB reports as the RAPID.
- **Where it sits inside the window** is the round-trip delay, which sets the TA: early in the window means a near UE, late means a far UE.

The eNB returns both the RAPID and the TA to the UE in **Msg2, the Random Access Response (RAR)**.

Why does a late preamble look like the next-**lower** preamble rather than the next-higher one? Each preamble is the root sequence advanced by $v \times N_{cs}$ (the cyclic shift $C_v = v \times N_{cs}$ in TS 36.211 §5.7.2). Propagation delay undoes part of that advance, so a delayed preamble looks like the one below it. Our srsRAN simulations confirm it: a preamble 17 sent from beyond range was detected as preamble 16.



Blue = measured TA · Gray dashed = true delay · Red = TA wrongly reported from the start of the wrong window

Figure 2. Correlator output for four UEs that all send preamble 17. Windows run P17, P16, P15 from left to right, the order a correlator plots them by lag.

Assumes the unrestricted preamble set. A root's first preamble ($v = 0$) wraps to that root's last cyclic shift rather than a lower preamble number. Sources: 3GPP TS 36.211 §5.7.2; TS 38.211 §6.3.3.1; srsRAN 4G PRACH detector simulations, September 2026.

Figure 2 walks through four cases:

- **Near UE:** the spike lands early in P17. The eNB reports RAPID 17 and a small TA. Correct.
- **Far UE within range:** the spike lands late in P17. RAPID 17 and a large TA. Correct.
- **UE at 1.5x the Ncs range:** the delay passes the end of the P17 window, so the spike lands mid-window in P16. The eNB reports RAPID 16 and a mid-range TA.
- **UE at 2.1x the Ncs range:** the spike passes two windows and lands early in P15. The eNB reports RAPID 15 and a **small** TA, even though the UE is far away.

The critical point is that **the eNB measures TA from the start of the window it believes the spike belongs to**. It has no way to know which preamble the UE actually sent, so it has no way to know the delay has “wrapped”. Checking the RAPID is the UE’s job, not the eNB’s.

THE CORE CONCEPT

Grounded in the 3GPP standards, this is how a TA short throw can happen: a UE beyond the Ncs range produces a spike in the wrong window, and the eNB faithfully measures and reports a short TA from that window.

6. What the Phone Does with a Mismatched RAPID

The UE retries until it runs out of attempts

Msg2 lists each RAPID the eNB detected in that PRACH opportunity, with a TA and an uplink grant for each. The UE looks for the RAPID of the preamble it sent:

- **Match:** the UE applies the TA and sends Msg3, the RRC Connection Request. Access continues.
- **No match:** the UE ignores the RAR, as if it had received no response at all. The procedure stops there and never reaches Msg3.

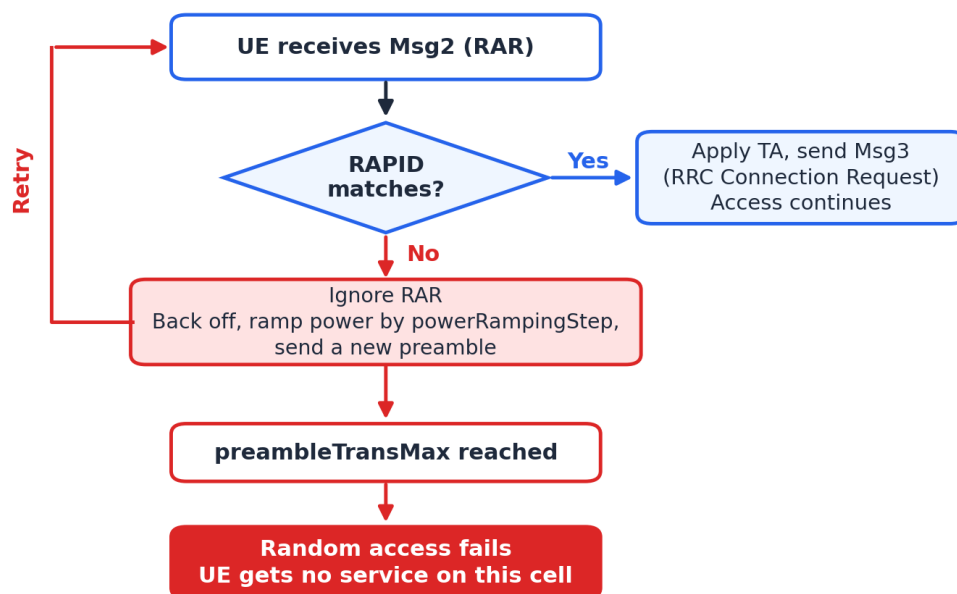


Figure 3. What the UE does with Msg2. A match leads to Msg3; a mismatch leads to backoff, a power increase and a new preamble, up to preambleTransMax.

After a mismatch the UE retries. It waits a random backoff (if the RAR carried a Backoff Indicator), raises its transmit power by powerRampingStep and sends a new preamble. The UE cannot retry forever, because unlimited retries could flood the PRACH and interfere with other UEs. Each attempt counts toward **preambleTransMax**, which the UE learned from SIB2; a setting on the order of 8 to 10 attempts is common. At the limit, the MAC layer reports a random access problem to RRC, and the UE gets no service on that cell.

A Backoff Indicator does not end the retries. It only tells the UE how long to wait before the next one. The limit that ends them is preambleTransMax.

A UE beyond the Ncs range fails every retry the same way. More power does not fix a timing problem. The result is a UE that cannot access the cell, even though the eNB may have detected and measured each of its preambles.

7. Cell Range Limits Only New Access

Once connected, the eNB keeps the UE's timing with TA commands

Everything so far concerns **access**, meaning the random access (RACH) procedure. Cell range sets how late a preamble can arrive and still be decoded as the right RAPID. The RACH procedure only sets the initial TA. Once the connection is established, the eNB tracks the UE's timing with **MAC TA commands**, adjusting as the round-trip delay grows. At that point the configured cell range is a long-forgotten byproduct of the RACH procedure.

So a UE that connects inside the cell range **can drive past it and keep service**, as long as the rest of the connection holds up. Connected-mode limits are coverage-based: handover thresholds (events A3 and A5 on RSRP or RSRQ) and radio link failure timers (T310 and N310). TA has its own ceiling of about 100 km (a maximum RAR TA of 1,282 steps × 0.52 μs).

Table 7. Distance from the eNB: what still works

	Inside cell range	Beyond cell range, inside coverage	Beyond coverage edge
New access (RACH)	Yes	No	No
Connected UE stays on	Yes	Yes	No
Timing kept by	RAR TA	MAC TA commands	—

The catch is that **any new RACH beyond the cell range fails**, so the UE loses service the moment it needs to re-access. Beyond the cell range, these re-access cases fail:

- Handover into this cell from a neighbor
- RRC re-establishment after a radio link failure (a dropped call)
- Uplink resynchronization after the timeAlignmentTimer expires, because a TA is not valid forever and a stale TA forces a new access attempt
- Going idle, then trying to connect again

8. Worked Examples: 10 km and 25 km

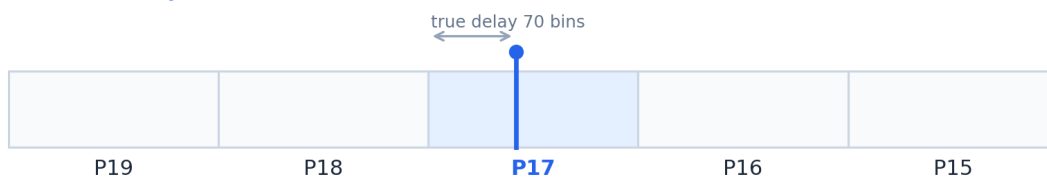
The same cell and preamble; only the distance changes

The two examples below use one cell configuration and one preamble. In the first, the UE is well inside the cell range and everything works. In the second, the UE is just beyond it.

Table 8. Example cell configuration

Item	Value
prach-ConfigIndex	35: preamble format 2 (2 ms, subframes 1–2), PRACH in subframe 1 of any frame
zeroCorrelationZoneConfig	13: $N_{cs} = 167$, a cell range of about 23.1 km
rootSequenceIndex	0 (assumed). Logical root 3 maps to $u = 699$; with 5 preambles per root, preambles 19 to 15 share it
Preamble sent	17, picked at random from 0–63. Cyclic shift $C_v = 2 \times 167 = 334$
RA-RNTI	$1 + t_{id}(1) + 10 \times f_{id}(0) = 2$
Payload	None. The sequence itself is the ID

UE at 10 km: peak at bin 70, inside window 17 → RAPID 17, TA 128 (≈10.0 km)



UE at 25 km: peak at bin 175, 8 bins into window 16 → RAPID 16, TA 15 (≈1.2 km)



Correlator output for root $u = 699$, $N_{cs} = 167$, in lag order (the axis wraps; 4 unused bins sit between P15 and P19).

Figure 4. Correlator output for the two examples. At 10 km the peak stays inside window 17. At 25 km it crosses N_{cs} and lands 8 bins into window 16.

Table 9. Side-by-side results

	UE at 10 km	UE at 25 km
Round-trip delay	66.7 μ s	166.8 μ s
Delay in bins (0.954 μ s each)	70	175
Inside Ncs 167?	Yes	No: 8 bins over
Inside format 2 guard time (197 μ s, 29.5 km)?	Yes	Yes, so the format is not the problem
Window hit, reported RAPID	17	16
TA in the RAR (11 bits)	128 (000100000000)	15 (00000001111)
Distance implied by the TA	$\approx$ 10.0 km	$\approx$ 1.2 km (true TA would be 320)
What the UE does	RAPID matches: applies TA 128 and sends Msg3	RAPID 16 $\neq$ 17: ignores the RAR, retries and fails the same way until preambleTransMax

The arithmetic for the 25 km case: the 175-bin delay exceeds Ncs 167, so the peak lands 8 bins into window 16. Eight bins is 7.6 μ s, and 7.6 μ s $\div$ 0.521 μ s per TA step gives a TA of 15, about 1.2 km. The TA the UE actually needed was 320.

Both RARs are 6-byte MAC RARs, sent on the PDSCH and found through the PDCCH using RA-RNTI 2. Each carries a MAC subheader with the RAPID, followed by the TA command, a 20-bit uplink grant telling the UE where to send Msg3, and a 16-bit Temporary C-RNTI that identifies the UE until contention resolves.

WHAT THE ENB SEES AT 25 KM

A clean peak for preamble 16 from a UE about 1.2 km away. **Nothing flags an error. It's the UE's responsibility to reject the RAR message with the incorrect (i.e. offset RAPID).**

9. Reproducing It in Simulation with srsRAN

A real LTE PRACH detector, run on a laptop

Because short throws are so hard to catch in the field, simulation is the best tool available today for testing the theory. **srsRAN 4G**, built and published as open source by Software Radio Systems (SRS), a wireless software company working since 2012, is a complete LTE network in software: UE, eNodeB and core. Labs pair it with software radios to run real test cells.

For this work, what matters is that srsRAN's eNodeB contains a **real PRACH detector**. It correlates the preamble, picks the Ncs window and turns the peak offset into a TA: exactly the chain described in Sections 4 through 8. We built a small test program on srsRAN's PRACH library. No radio, phone or live network is involved. The program lets us step the delay past the Ncs limit and watch the RAPID change and the TA collapse, which is nearly impossible to reproduce on a live cell in a commercial network.

Table 10. The PRACH lab: one preamble, one delay, one detection

Step	What happens
1 Generate	srsRAN builds preamble 17 from the SIB2 settings: config index, Ncs and root.
2 Delay	The test shifts it by d samples. 1 sample = 0.521 μ s $\approx$ 1 TA step $\approx$ 78 m.
3 Detect	srsRAN's eNodeB correlator finds the peak and the Ncs window it lands in.
4 Report	It prints the detected preamble (the RAPID Msg2 would carry) and the TA.

We ran the same cell and preamble twice: config index 35 (format 2), Ncs 167, root 22, with the UE sending preamble 17. Only the injected delay changed, from 10.0 km to 25.8 km, against an Ncs window of 159.2 μ s (about 23.9 km before delay spread).

Table 11. srsRAN prach_lab results

	Run 1: UE at 10.0 km	Run 2: strong peak (UE at 25.8 km)	Run 2: weak peak (same run)
Delay injected	66.7 μ s (128 samples)	171.9 μ s (330 samples)	—
Detected preamble	17	16	17
Timing offset	66.7 μ s	12.4 μ s	157.3 μ s
TA command	128	23	302
Apparent distance	10.0 km	1.9 km	23.6 km
Peak / average	752	530	36
Preamble match	Yes	No	Yes

Source: srsRAN 4G prach_lab runs, -d 128 and -d 330, September 2026. 1 sample = 0.521 μ s. Console output and setup details are available on request.

Run 1 behaves exactly as expected: a strong peak (752) in window 17, RAPID 17 and TA 128. In Run 2, the leftover delay lands in window 16: 171.9 μ s of delay minus the 159.2 μ s Ncs window leaves 12.6 μ s, and srsRAN measured 12.4 μ s in window 16, one below the 17 the UE sent. **The strong peak wins: RAPID 16, TA 23, an apparent distance of 1.9 km.** The UE sent 17, so it would ignore that RAR entry.

Run 2 also shows something interesting. The detector still sees a much weaker peak for preamble 17 (36, compared with 530), sitting at the far edge of its window with a TA of 302. Whether a real eNB would also answer that weaker peak depends on its detection threshold. 3GPP does not dictate the threshold; it sets detection performance requirements that vendors must meet (TS 36.104). If an eNB did report both, the UE would discard RAPID 16 and accept RAPID 17 with a TA near the window edge. That makes a short throw that coincides with a successful access rarer still.

A LEARNING TOOL, NOT EVIDENCE

Clean channel, one UE, physical layer only. The results show what the 3GPP math produces, not how any operator's eNodeB is configured or behaves in the field.

10. Why Short Throws Are Rare

Operators size cells to avoid failed access

From an operator's perspective, **there is no incentive to set a cell range too small**. A range that is too small shows up as failed access attempts in the operator's own key performance indicators, and every operator targets 100% access success. Those metrics drive customer satisfaction, internal performance targets and network-quality rankings, so undersized cells get noticed and fixed *quickly*!

The author recalls a rural site more than a decade ago that was turned up with default cell range settings (usually good enough at the time, during early commercial LTE deployments). Its access success rate was only about 30%. It was caught quickly in the statistics, the cell range was increased, and access success immediately improved to nearly 100%. Figure 5 illustrates that pattern.

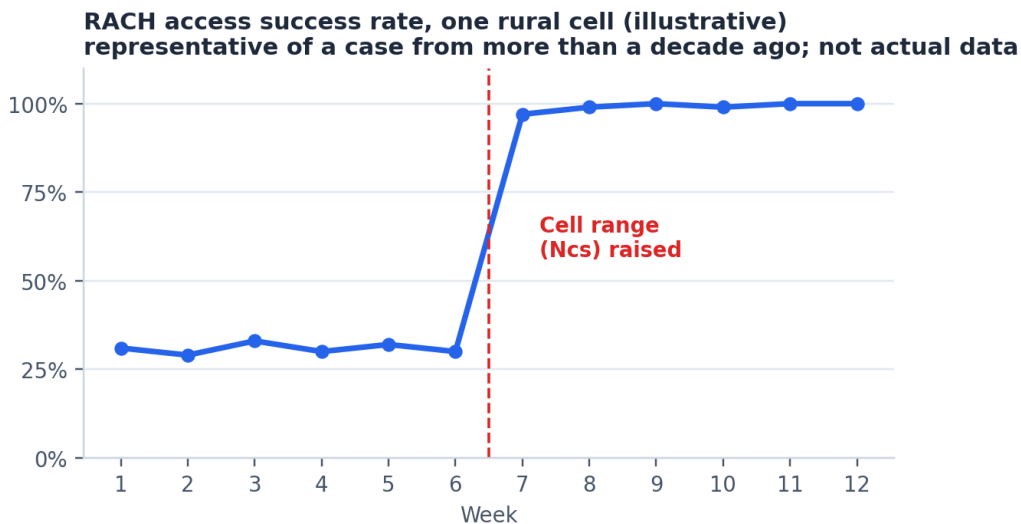


Figure 5. RACH access success rate for one rural cell, by week. A representative illustration, not actual data.

So why not set every cell to the maximum range? **Capacity**. A larger Ncs yields fewer preambles per root, so each cell needs more root sequences and neighbors must reuse them sooner. LTE has 838 root sequences. At the smallest Ncs, one root yields all 64 preambles and 838 cells can each have their own. At the 59.1 km setting, only 26 cells get unique roots before reuse. In a dense urban network with hundreds or even thousands of time-synchronized sites, that would mean PRACH collisions everywhere. Setting every cell to 1 km fails the other way: no one beyond 1 km can access the network. Both scenarios would be equally bad.

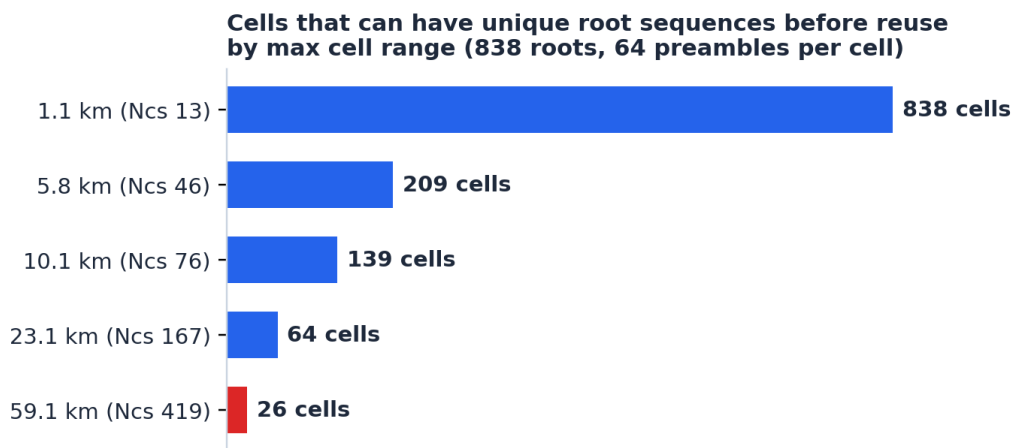


Figure 6. Cells that can have unique root sequences before reuse, by maximum cell range (838 roots, 64 preambles per cell).

Cell range is always a balancing act, and operators are strongly motivated to get it right. Advanced networks also tune Ncs automatically with self-organizing network (SON) features, so the issue gets rarer every year. In practice:

- **Dense urban: extremely rare.** Cells are small, so UEs sit well inside even the smaller Ncs ranges.
- **Rural: worth checking.** Large cells and long line-of-sight paths are where a UE can end up beyond the configured range. Worth checking, but still extremely rare.

11. What This Means for Investigators

When to consider short throws, when to rule them out

The mechanism in this paper gives investigators a way to reason about short throws rather than simply distrust long-range TA. The following points summarize how to apply it.

THE RECORDS KEEP THEIR INTEGRITY

A short-throw TA is the TA the eNB actually measured, recorded exactly as designed. No export error or data-pipeline fault is needed to explain it. With this understanding, there is no need to debate the integrity of the operator's data on this point. The task is reading the records correctly.

ESTABLISH THE CONFIGURED CELL RANGE

Capture SIB2 at the site and read `zeroCorrelationZoneConfig` and `prach-ConfigIndex`. Look up the Ncs range and the format range, and take the lower value. This tells you the distance beyond which a new access attempt can produce a short throw.

CONSIDER THE ENVIRONMENT

In dense urban areas, short throws are extremely unlikely because UEs sit well inside even small cell ranges. In rural areas with large cells and long line-of-sight paths, a UE beyond the configured range is plausible and the possibility deserves attention.

UNDERSTAND WHAT A SHORT THROW REPRESENTS

By this mechanism, a short-throw TA comes from a **failed access attempt**: the UE sent a preamble from beyond the cell range, received a mismatched RAPID and did not proceed to Msg3 on that attempt.

A UE that connected inside the range and then moved beyond it keeps accurate timing through MAC TA commands and does not produce a short throw by this mechanism.

WORK OUT WHERE THE PHONE COULD ACTUALLY BE

Because the eNB measures the leftover delay after the spike wraps into a lower window, the true distance is approximately the TA-implied distance plus a whole number of Ncs window lengths. In the 25 km example, a TA-implied 1.2 km plus one 23.9 km window (Ncs 167, before delay spread) gives about 25.1 km. Candidate distances should be treated as possibilities to test against other evidence, not as locations.

GET HELP WHEN IT MATTERS

If you are working a case where a short TA may be in play, Wireless Architect Group can help apply these concepts to your records. See the last page for contact details.

12. Confirming the Theory: A Call for Partners

The theory follows from the 3GPP standards; field captures would confirm it

We are confident in this explanation, based on the standards, the simulations and more than 20+ years of wireless industry experience. But the effect is rare and hard to reproduce, and we have not yet captured it in the field ourselves. It is not for lack of trying. Our goal is to **validate in the field, with live eNB captures, how the cell range setting decides whether a distant UE gets access.**

WHAT THE TEST GEAR MUST CAPTURE

Confirmation requires test equipment that decodes **Msg2 (the RAR) from the eNB**, specifically the RAPID and TA values it sends back. Our current drive gear does not do this, and it is likely an area that requires high-end test equipment.

Table 12. Data needed for each access attempt

Field	Where it comes from	Why it matters
RAPID	Msg2 (RAR) MAC subheader	Which preamble the eNB heard
TA	Msg2 (RAR) payload	The delay the eNB measured
Preamble sent	UE-side log of Msg1	Shows whether the RAPID matches
Ncs and PRACH config index	SIB2	The configured cell range
True UE distance	GNSS position and site location	The ground truth to compare against

Comparing each RAPID and TA with the UE's true distance shows exactly when and why access fails beyond the configured range. We propose to work together in three steps: **capture** Msg1 and Msg2 at known distances from the site, **compare** the RAPID and TA against the true distance, and **share** the method and results together. We offer a partnership in which the method, the analysis and the credit for the results are shared.

A PROPOSED TEST RIG: SHORT THROWS ON DEMAND

Because operators work to prevent this effect, it rarely shows up in the field. A test rig would make it happen on demand. Two RF-over-fiber modules are connected by a 15–30 km fiber spool, and the UE sits in a Faraday box so that its only path to the eNB runs through the fiber. The whole setup is stationary and repeatable: swap or daisy-chain spools to step the delay past the cell range, and log the RAPID and TA each time.

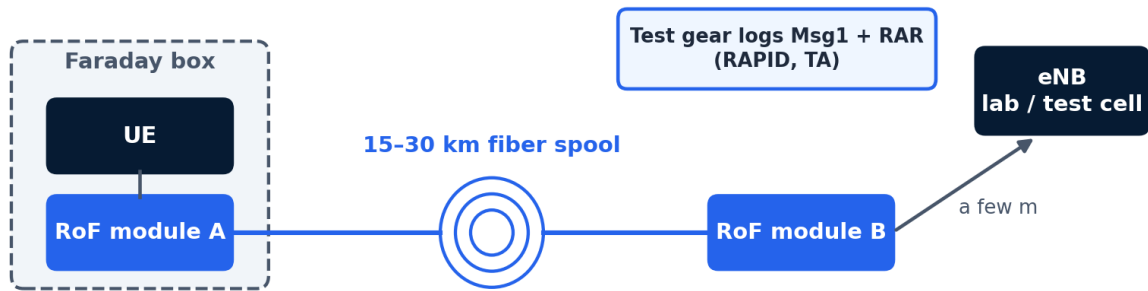


Figure 7. Proposed test rig: the delay lives in a fiber spool, so the UE can be made to look far away without moving.

Light travels more slowly in fiber than in air (refractive index $n \approx 1.47$, about $4.9 \mu\text{s}$ per km each way), so fiber distance looks longer to the eNB than it is. 15 km of fiber adds about $147 \mu\text{s}$ of round-trip delay, the same as a UE 22 km away.

Table 13. What the eNB would see (Ncs 167, 23.1 km cell range)

Fiber	Round trip	Looks like	Expected result
0 km	$\sim 0 \mu\text{s}$	Next to the site	Correct RAPID
15 km	$147 \mu\text{s}$	22 km	Correct RAPID
20 km	$196 \mu\text{s}$	29 km	Wrong RAPID
30 km	$294 \mu\text{s}$	44 km	Wrong RAPID or none*

Air-equivalent distance = fiber km $\times$ 1.47. *The format 2 guard time caps range at 29.5 km, so at 44 km the eNB may report a wrong RAPID or nothing at all.

Stay legal. The rig must run against a lab eNB or an operator-approved test cell, never unlicensed on live spectrum. The RF-over-fiber modules and fiber need funding, but the cost is modest by RF-industry standards.

HAVE GEAR THAT DECODES THE RAR? LET’S PARTNER.

If you have RF-over-fiber equipment, fiber, a lab eNB, a test license or test gear that decodes Msg2, or can help fund the study, please contact Wireless Architect Group. We would like to turn this from a mysterious, untrusted effect into data the whole community understands and can rely on.

13. Conclusion

TA short throws are real, and the LTE standards explain them. A UE that tries to access a cell from beyond its configured Ncs range produces a correlation spike in the wrong preamble window. The eNB reports the wrong RAPID and measures a short TA from that window, and the UE, seeing the mismatch, never completes access on that cell. The network is working as designed, and the operator's records faithfully reflect what the eNB measured.

For investigators, that turns an unexplained anomaly into something that can be reasoned about. The configured cell range can be read directly from SIB2. The environments where short throws are plausible can be identified. And the records themselves remain trustworthy. What remains is field confirmation, and we invite partners to help us complete it.

References

STANDARDS

- [1] **3GPP TS 36.211: E-UTRA physical channels and modulation.** PRACH preamble formats (Table 5.7.1-1), PRACH configuration index (Table 5.7.1-2), Ncs (Table 5.7.2-2), ZC length 839, cyclic shift $C_v = v \times N_{cs}$ (§5.7.2).
- [2] **3GPP TS 36.213: E-UTRA physical layer procedures.** Random access procedure, TA command, 16 Ts TA step (≈ 78 m).
- [3] **3GPP TS 36.321: E-UTRA MAC protocol.** RAR format (RAPID, TA), Backoff Indicator, preambleTransMax, TA commands.
- [4] **3GPP TS 36.331: E-UTRA RRC protocol.** MIB, SIB1 and SIB2 PRACH parameters, handover events, T310 and N310.
- [9] **3GPP TS 38.211: NR physical channels and modulation.** PRACH cyclic shift definition (§6.3.3.1).
- [10] **3GPP TS 36.104: E-UTRA base station radio transmission and reception.** PRACH detection performance requirements.

PAPERS, BOOKS AND SOFTWARE

- [5] **Forensic Analytics: “Timing Advance Short Throws: What Recent Evidence Really Tells Us” (whitepaper and blog, March 2026).** <https://www.forensicanalytics.io/us/knowledge-hub/timing-advance-short-throws-what-recent-evidence-really-tells-us/>. Accessed August 2026.
- [6] **C. Johnson: Long Term Evolution in Bullets, 2nd ed..** PRACH configuration index table (Table 348).
- [7] **srsRAN 4G: open-source LTE software stack.** PRACH generator and detector (lib/src/phy/phch/prach.c), github.com/srsran/srsRAN_4G; Software Radio Systems, srsran.com. Used for the PRACH delay simulations, September 2026.

Appendix A: PRACH Configuration Index (FDD)

Read prach-ConfigIndex from SIB2, find it here, and pair the format with Ncs

Idx	Fmt	Dens.	SFN	Subframes	Idx	Fmt	Dens.	SFN	Subframes
0	0	0.5	Even	1	32	2	0.5	Even	1
1	0	0.5	Even	4	33	2	0.5	Even	4
2	0	0.5	Even	7	34	2	0.5	Even	7
3	0	1	Any	1	35	2	1	Any	1
4	0	1	Any	4	36	2	1	Any	4
5	0	1	Any	7	37	2	1	Any	7
6	0	2	Any	1, 6	38	2	2	Any	1, 6
7	0	2	Any	2, 7	39	2	2	Any	2, 7
8	0	2	Any	3, 8	40	2	2	Any	3, 8
9	0	3	Any	1, 4, 7	41	2	3	Any	1, 4, 7
10	0	3	Any	2, 5, 8	42	2	3	Any	2, 5, 8
11	0	3	Any	3, 6, 9	43	2	3	Any	3, 6, 9
12	0	5	Any	0, 2, 4, 6, 8	44	2	5	Any	0, 2, 4, 6, 8
13	0	5	Any	1, 3, 5, 7, 9	45	2	5	Any	1, 3, 5, 7, 9
14	0	10	Any	0 to 9	46	2	N/A	—	—
15	0	0.5	Even	9	47	2	0.5	Even	9
16	1	0.5	Even	1	48	3	0.5	Even	1
17	1	0.5	Even	4	49	3	0.5	Even	4
18	1	0.5	Even	7	50	3	0.5	Even	7
19	1	1	Any	1	51	3	1	Any	1
20	1	1	Any	4	52	3	1	Any	4
21	1	1	Any	7	53	3	1	Any	7
22	1	2	Any	1, 6	54	3	2	Any	1, 6
23	1	2	Any	2, 7	55	3	2	Any	2, 7
24	1	2	Any	3, 8	56	3	2	Any	3, 8
25	1	3	Any	1, 4, 7	57	3	3	Any	1, 4, 7
26	1	3	Any	2, 5, 8	58	3	3	Any	2, 5, 8
27	1	3	Any	3, 6, 9	59	3	3	Any	3, 6, 9
28	1	5	Any	0, 2, 4, 6, 8	60	3	N/A	—	—
29	1	5	Any	1, 3, 5, 7, 9	61	3	N/A	—	—
30	1	N/A	—	—	62	3	N/A	—	—
31	1	0.5	Even	9	63	3	0.5	Even	9

Density = PRACH opportunities per 10 ms radio frame. Indices 30, 46, 60, 61 and 62 are not supported because their preambles would overlap in time. Source: 3GPP TS 36.211, Table 5.7.1-2.

Appendix B: Key Constants and Formulas

The numbers behind the examples

Quantity	Value or formula
Basic time unit (Ts)	$1 \div (15,000 \times 2,048) \text{ s} \approx 32.55 \text{ ns}$
TA step	$16 \text{ Ts} \approx 0.521 \mu\text{s} \approx 78.1 \text{ m of distance}$
Distance from TA	$\text{TA} \times 78.1 \text{ m (for example, } 128 \times 78 \text{ m} \approx 10.0 \text{ km)}$
PRACH correlation bin	$800 \mu\text{s} \div 839 \approx 0.954 \mu\text{s}$
Ncs range	$(\text{Ncs} \times 800/839 \mu\text{s} - \text{delay spread}) \times c \div 2$
Preamble format range	$\text{Guard time} \times c \div 2$

Quantity	Value or formula
Cell range	Lower of the Ncs range and the preamble format range
Preambles per root	$\lceil 839 \div \text{Ncs} \rceil$
Roots needed per cell	$\lceil 64 \div \text{preambles per root} \rceil$
Cyclic shift of preamble v	$C_v = v \times \text{Ncs}$ (unrestricted set)
Maximum RAR TA	1,282 steps $\approx$ 100 km
Fiber delay	$n \approx 1.47$, about 4.9 μs per km each way; air-equivalent = fiber km $\times$ 1.47

Appendix C: Glossary

Term	Meaning
eNB (eNodeB)	The LTE base station. In 5G NR the equivalent is the gNB.
UE	User equipment: the phone or other device.
RACH / PRACH	Random access channel (the procedure) and physical random access channel (the radio resource it uses).
Msg1	The random access preamble the UE sends to start access.
Msg2 (RAR)	Random Access Response from the eNB, carrying the RAPID, TA, uplink grant and Temporary C-RNTI.
Msg3	The UE's first scheduled uplink message, such as the RRC Connection Request.
RAPID	Random Access Preamble ID: the index (0–63) of the preamble the eNB detected.
Zadoff-Chu (ZC) sequence	The 839-sample sequence from which LTE preambles are built.
Ncs	Cyclic shift size. Sets both the spacing between preambles and each preamble's arrival window.
zeroCorrelationZoneConfig	The SIB2 integer (0–15) that selects Ncs.
prach-ConfigIndex	The SIB2 integer (0–63) that implies the preamble format and PRACH timing.
preambleTransMax	Maximum number of preamble attempts before random access is declared failed.
Timing advance (TA)	The timing correction that aligns a UE's uplink; proportional to round-trip delay.
TA short throw	A recorded TA far shorter than the UE's true distance from the site.
SIB2	System Information Block 2, which carries the random access and cell range parameters.

About Wireless Architect Group

Training, analytics, and software for investigators

Wireless Architect Group

“Investigators shouldn’t need a PhD in engineering to rely on network data relevant to their investigations. Our mission is to bridge that gap.”

Who we are. Wireless Architect Group helps investigators, analysts and attorneys understand and use the 4G and 5G network data behind their evidence.

What we teach. How the network works, from the radio link to the records it produces, explained without the engineering jargon. Courses run from beginner to advanced, online and in person, and tie back to the data investigators use, such as timing advance and cell site records.

Beyond training. Network analytics on operator records, case reviews, consulting and custom software solutions built around an agency’s workflow.

Course topics: TA measurement analysis · 4G LTE · 5G NR

We always offer a free scoping call to see whether we are the right fit.

WirelessArchitectGroup.com · reggie@wirelessarchitectgroup.com