A Case for Stateless Mobile Core Network Functions in Space

ACM SIGCOMM'22 submission #165, 12 pages + references + appendices

ABSTRACT

Is it worth and feasible to push mobile core network functions to low-earth-orbit (LEO) satellite mega-constellations? While this paradigm is being tested in space and promises new values, it also raises scalability, performance, and security concerns based on our study with datasets from operational satellites and 5G. A major challenge is today's *stateful* mobile core, which suffers from signaling storms in satellites' extreme mobility, intermittent failures in outer space, and attacks when unavoidably exposed to untrusted foreign locations. To this end, we make a case for a *stateless* mobile core in space. Our solution, SpaceCore, decouples states from orbital core functions, simplifies location states via geospatial addressing, eliminates unnecessary state migrations in satellite mobility by shifting to geospatial service areas, and localizes state retrievals with device-as-the-repository. Our evaluation with datasets from operational satellites and 5G shows SpaceCore's 17.5× signaling reductions and resiliency to failures/attacks compared to existing solutions.

1 INTRODUCTION

Mobile networks (5G and beyond) have successfully served billions of users. But their heavy deployment and operation costs (10s–100s billions of dollars [1, 2]) in rural areas, developing countries, aircraft, or oceans limit them to cover the remaining 3.7 billion global users [3]. Their fixed deployment limits regional operators to expand to international services for more revenues. Their terrestrial infrastructure is also vulnerable to disasters (earthquakes, tornados, or wars).

Pushing mobile networks to space is a promising solution to these issues. Satellite communications via 2G–5G have been operational for decades [4–11]. They complement terrestrial networks' coverage to remote areas at lower costs. The recent low-earth-orbit (LEO) satellite mega-constellations (Starlink [12], OneWeb [7], Amazon Kuiper [13], Boeing [14], and more) further promise competitive bandwidth and latency to terrestrial networks. To this end, the industry is actively extending 5G (and beyond) to LEO constellations with standardizations [15–18] and early adoptions [19–24].

Early mobile satellites are standalone, transparent physical pipes in the geostationary orbit with broad coverage and low performance (Figure 1a). In LEO mega-constellations, this model suffers from low coverage and single-point bottlenecks [25, 26]. Instead, operators and infrastructure vendors have started to experiment LEO satellites as 5G radio access

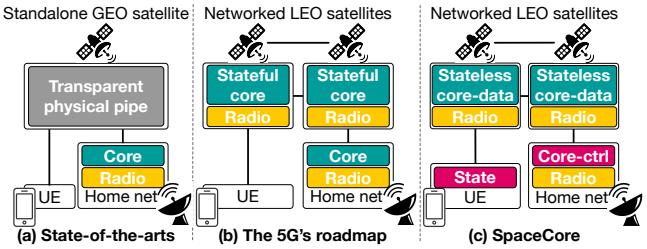


Figure 1: Mobile function and state divisions in space.

[19–21] and core network [22–24, 27] functions (Figure 1b). This paradigm, if feasible, could solve the above issues *and* potentially boost new values like global mobile service expansions, seamless space-terrestrial 5G integration, lightweight satellite devices, and orbital edge computing [28–32] (§2.2).

Despite so, pushing mobile core functions to space is still controversial. Unlike fixed terrestrial infrastructure, LEO satellites move fast in the unreliable, untrusted outer space at the global scale. This challenges basic assumptions in mobile networks. In §3, we analyze various options of pushing mobile core to space based on our signaling datasets from operational satellites and terrestrial 5G (Table 2)[1]. If placed in LEO satellites, today's mobile core can suffer from signaling storms (10^4 signaling/s per satellite, 10^5 signaling/s per ground station), repetitive mobility registrations for numerous *static* users (every 165.8s), service disruptions in space failures [33–35], and sensitive state leakages (e.g., security keys) in satellite attacks [36–40]. These issues are exacerbated with more satellites and users served by each satellite.

We show these issues are rooted in the *stateful* mobile cores today. To offer carrier-grade services, the mobile network establishes sessions between user equipment (UE) and infrastructure with states of traffic delivery, mobility, QoS, billing, and security. As the UE moves, the core migrates these states to the new infrastructure node to retain continuous services. These state operations must succeed before activating data services. While feasible for fixed terrestrial infrastructure, this design incurs excessive state migrations in LEO satellite mobility for *static* UEs. These state migrations are vulnerable to intermittent failures that are not uncommon in space (≈3% in Starlink [33]). Moreover, the stateful orbital core is exposed to untrusted foreign locations and thus threatened by attacks and sensitive state leakages (e.g., security keys). This issue also demotivates applying recent optimizations of proactive state replications [41–43] to space.

To this end, we make a case for a *stateless* mobile core in space. The basic idea is simple: Decouple core functions from

[1]We plan to release our satellite and 5G signaling dataset upon acceptance.

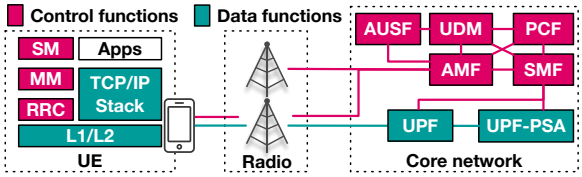


Figure 2: Terrestrial mobile network functions in 5G.

states to mitigate the above exhaustive state migrations, failures, and attacks in LEO satellites. The challenge, however, is how to retain carrier-grade services after the function-state decoupling. This results in three fundamental questions:

Q1: *What* session states are "must-haves" for orbital core?

Q2: *Where* are these states placed (if not in satellites)?

Q3: *How* can orbital core functions work with these states?

SpaceCore solves Q1–Q3 with *localized, geospatial state management*. Its key insight is that the *local UEs* naturally form a scalable, resilient, secure state repository for the fast-moving satellites. SpaceCore utilizes this readily available feature to decouple states from orbital core, simplify location states via geospatial addressing, eliminate state migrations in satellite mobility by shifting to *geospatial* service areas, and localize state retrievals with device-as-the-repository. SpaceCore is decentralized without bottlenecks from space-terrestrial asymmetry, and lightweight for LEO satellites. It supports seamless integration with terrestrial 5G and commodity UEs.

We prototype SpaceCore with open5gs [44] on commodity hardware used by 5G LEO satellites. Compared to existing solutions, SpaceCore reduces 17.5×–122.2× signaling costs, removes bottlenecks from remote gateways, and is resilient to satellite failures/attacks in exposed foreign locations.

Ethics: This work does not raise any ethical issues.

2 MOTIVATION

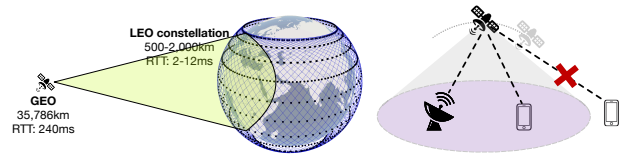
We introduce the terrestrial mobile network (§2.1) and motivate why and how it is currently expanded to space (§2.2).

2.1 Terrestrial Mobile Networks

The mobile network (5G and beyond) is the largest terrestrial wireless infrastructure for wide-area data access. It consists of the radio access network and core network (Figure 2). The radio access network offers wireless services to user equipments (UEs, such as phones and IoT devices) with base stations. The core network relays traffic between base stations, and runs diverse functions for carrier-grade services, such as user profile management, authentication, mobility control, session management, policy control, traffic forwarding, and anchor gateway[2]. These functions interacts with each other in the distributed environment via signaling exchanges (§3).

The mobile network tracks a UE's location and service by its two-tier *service areas*. At the fine granularity, each base station runs one or more small service areas called *cells*. As the UE moves, the serving cell migrates its service to the new cell via *handover*. At the coarse granularity, base stations are grouped as a larger *tracking area* (managed by an AMF). When crossing tracking areas, the UE updates its new location to the core via *mobility registration update* (§3.2).

[2]In 5G jargons, they are called UDM, AUSF, AMF, SMF, PCF, UPF, and PDU session anchor UPF (PSA-UPF) [45–50]. See Appendix B for the acronyms.



(a) GEO orbit vs. LEO orbit (b) Transparent pipe

Figure 3: Coverage of standalone mobile satellites.

	Satellites per orbit n	Total orbits m	Total satellites $n \cdot m$	Altitude H (km)	Inclination angle ϕ	Speed
Starlink [12]	22	72	1,584	550	53°	7.6 km/s
OneWeb [7]	40	18	720	1,200	87.9°	7.3 km/s
Kuiper [13]	34	34	1,156	630	51.9°	7.5 km/s
Iridium [53]	11	6	66	780	86.4°	7.4 km/s

Table 1: LEO satellite mega-constellations today.

(a) Baoyun LEO satellite as 5G core + orbital edge [22–24, 27] (b) Satellite devices in our tests

Figure 4: Mobile communication satellites & devices.

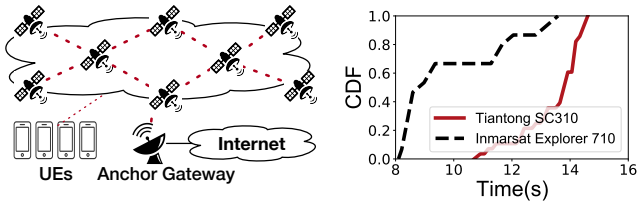
2.2 Mobile Satellites Today & Limitations

A satellite can run at geostationary orbit (GEO, at the altitude of ≈ 35,786 km) or non-geostationary orbit, such as low-earth orbits (LEO, ≤2,000 km). As shown in Figure 3a, LEO satellites promise shorter RTT and more bandwidth[3], but at the cost of lower coverage. So LEO mega-constellations are deployed for global coverage with 100s–1,000s of satellites (Table 1). LEO satellites have microwave radio for terrestrial users and inter-satellite links for networking in space.

Today, most satellite communications use 2G–5G mobile network technologies, such as OneWeb [7], Inmarsat [8, 9], Boeing [14], Iridium [6], Thuraya [11], and Tiantong [52]. They are classified into three categories by satellites' role:

Satellites as transparent pipes: This is the *de facto* mode for most satellites today. Satellites only relay physical radio signals between terrestrial nodes without further processing. In 2G GMR [4], 3G BGAN [54], 4G SES [5], and 5G NTN [15, 16], geostationary satellites (at 35,786 km altitude) relay the radio signals between devices (e.g., satellite phones) and terrestrial ground stations. Mobile operators also rent satellites from OneWeb [7, 55] or Starlink [56, 57] as backhauls to relay signaling/data traffic between base stations and core network, which saves their fiber deployments in rural areas.

[3]LEO Satellites and 5G are competing for millimeter wave spectrums [51].



(a) Ground stations as bottlenecks. (b) Registration signaling latency.

Figure 5: Bottlenecks by space-terrestrial asymmetry.

Trace 1 Session establishment in Inmarsat Explorer 710.

```
11:25:10.074 UMTS-GMM:Initiating service request
11:25:15.709 UMTS-GMM:Signalling connection secured
11:25:18.612 UMTS-GMM:Initiating RAU procedure
11:25:18.613 UMTS-MM:MM_LOCUPDPEND
11:25:18.615 UMTS-MM:MM_WAITRRLOCUPD
11:25:18.615 UMTS-MM:MM_LOCUPDINIT
11:25:19.264 UMTS-SM:AL State:DATA_CONN_ACTIVE
11:25:20.141 UMTS-GMM:Authentication request received
11:25:20.221 UMTS-SM:Qos:transferdelay:22, maxSDU:1500
11:25:20.221 UMTS-SM:Qos:bitRateUp:512/896, Down:512/896
11:25:20.222 UMTS-SM-GW:pdp new state Active
```

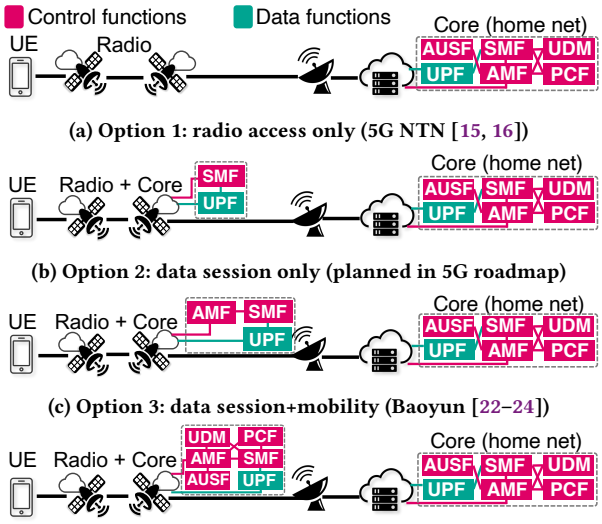
Early geostationary communication satellites are mostly standalone bent pipes to support local communications between nodes within their coverage (Figure 3). This is not effective for LEO satellites with small coverage [58]. Instead, modern LEO mega-constellations have adopted networked satellites to expand the coverage. Despite so, networked physical pipes suffer from bottlenecks from *space-terrestrial asymmetry*. As transparent physical links, satellites redirect all data and signaling to remote ground stations for further processing. Since remote ground stations are fewer than LEO satellites in mega-constellations, they become the bottleneck (Figure 5). At the data plane, [26] reports Starlink's ground stations determine the LEO network's total capacity despite mega-constellations. At the control plane, [59] shows Starlink ground stations should process 5 TB signaling traffic per day, and [25] reports each OneWeb's ground station must process 10,000 terminal handovers per second. From our experiments, Figure 5b and Trace 1 show 9.5s and 13.5s average registration delays in Inmarsat and Tiantong (detailed in §3). Such latency cannot meet 5G's stringent radio baseband processing (≤10 ms [60–63]) and signaling deadlines. Deploying more ground stations can alleviate this bottleneck, but lowers satellites' advantages over terrestrial networks.

Satellites as radio access: To alleviate both issues, recent efforts seek to offload mobile network functions to satellites. The first step is to let the satellite be the base stations with radio baseband processing (Figure 6a). This option has been used by satellites from Lockheed Martin [19], Lynk [20], and AST SpaceMobile [21], and standardized as the regeneration mode in 5G [15, 16]. It localizes radio processing to alleviate signaling delays and bottlenecks from ground stations.

Moreover, recent 5G radio satellites in [19–21] allow direct access by today's commodity smartphones without modifications (by faking as "terrestrial" base stations). This facilitates *lightweight* mobile devices without additional antennas or baseband chips for satellite communications.

	Mobile satellites			Terrestrial 5G		
	Inmarsat Explorer 710	Tiantong SC310	Tiantong T900	China Telecom	China Unicom	China Mobile
L1/L2	56,231	1,744,094	3,887,429	3,828,083	1,475,393	8,405,587
RRC	40,800	4,226	1,340	28,841	14,833	69,782
MM	57,264	43,555	12,626	605	970	4,194
SM	53,868	4,586	1,670	203	338	925
Others	762,957	310,455	376,671	0	0	0
Total	971,120	2,106,916	4,279,736	3,857,732	1,491,534	8,480,488

Table 2: Overview of dataset from our experiments.



(a) Option 1: radio access only (5G NTN [15, 16])

(b) Option 2: data session only (planned in 5G roadmap)

(c) Option 3: data session+mobility (Baoyun [22–24])

(d) Option 4: data session+mobility+security

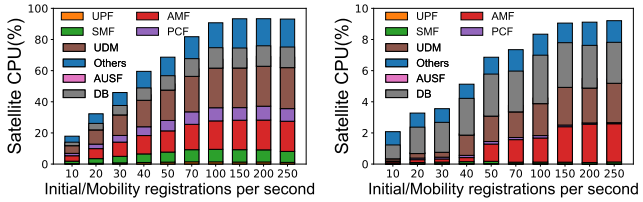
Figure 6: A taxonomy of core function splits in space.

However, satellites as radio access only do not suffice to eliminate bottlenecks from space-terrestrial asymmetry. First, link-layer radio access cannot route network data. All user traffic from satellites should still be relayed to the remote terrestrial home for forwarding (Figure 5). Second, splitting radio access and core functions between space and ground incurs new signaling storms as we will analyze in §3.1.

Satellites as core networks: On December 7, 2021, a LEO satellite called *Baoyun* (in *Tiansuan* orbital edge computing constellation [22–24, 27] from China Mobile, Huawei, and BUPT) was successfully launched and tested as a 5G core (Figure 4a and 6c). This satellite consolidates 5G mobility (AMF), session management (SMF), and user plane (UPF) functions. Satellites with radio and core network functions can potentially eliminate the above bottlenecks by routing traffic among satellites without ground stations and fully localizing signaling processing. They also promise new value propositions including (but not limited to):

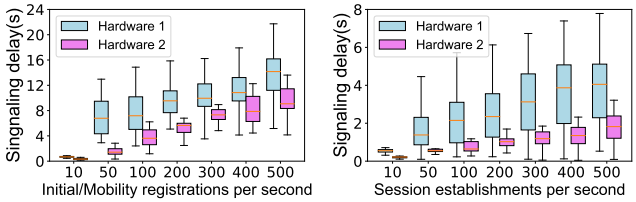
(1) Global service expansion: Satellites as core networks let regional operators seamlessly expand to international services *without* relying on competitive operators' expensive, slow, and sometimes untrusted foreign roaming [64].

(3) Orbital edge: Edge computing in LEOs has attracted interest from academia [31, 32, 65] and industry [28, 66–68]. It is beneficial to expand terrestrial CDNs to remote areas [13, 28, 31, 67], localize computations of earth observations



(a) Satellite hardware 1 [22–24] (b) Satellite hardware 2 [28, 74]

Figure 7: CPU usages by core network functions.



(a) Initial/mobility registration (b) Session establishment

Figure 8: Signaling latency in hardware by satellites.

[32, 65], empower space AI [66], and provide secure storage from space [68]. Orbital edge is made possible with the increasing powerfulness of satellite hardware. It needs space networking (thus orbital core functions) for functionality.

(3) Emergency communications: In disasters or wars, the terrestrial mobile infrastructure can be destroyed. In this case, satellites as radio and core functions can offer complementary services for emergency communications [41].

3 STATEFUL MOBILE CORE IN SPACE?

Unlike fixed terrestrial infrastructure, LEO satellites move fast in the unreliable, untrusted outer space at the global scale. This challenges today's *stateful* mobile core network functions. We study options of pushing stateful core to space and analyze their deficiencies in session establishment (§3.1), mobility (§3.2), and their resiliency to attacks/failures (§3.3).

Methodology: We analyze four options of orbital core from 3GPP standards [15, 16] and 5G satellites [22–24, 27] by progressively adding radio, session, mobility, and security functions to satellites (Figure 6). Rather than spread these functions to multiple satellites, we focus on consolidating them to each satellite that is coherent with today's 5G satellites [15, 16, 22–24] to save signaling costs [41, 42, 69]. We run what-if studies for each option by replaying datasets from operational satellites and terrestrial 5G (Table 2, collected by MobileInsight [70] and equipment in Figure 4b) and global mobile subscriptions [71] in ground stations in [72] (as home network) and LEO mega-constellations in Table 1 using grid topology [6, 73] and a testbed running open5gs [44] on two commodity hardware in real LEO satellites (detailed in §6).

Overview: Figure 9–8 compares orbital cores in Figure 6 in LEO mega-constellations. We make three observations:

(1) Exhaustive signaling storms: All options in Figure 6 incur signaling storms. Each LEO satellite must process $10^4 \sim 10^5$ signaling messages/s (depending on satellite capacity, location, and constellations). This cost is worsened at the ground stations by one order of magnitude due to space-terrestrial asymmetry (except for Option 4). It exhausts satellite hardware (Figure 7), congests ground stations and delays user services (Figure 8). Spreading functions to multiple satellites will incur even more signaling costs [41, 42, 69].

(2) Diverse causes of signaling storms: Without mobility functions in satellites (Figure 6a–6b), signaling storms arise from the stateful session establishment (§3.1). This deficiency can be alleviated by adding mobility functions to satellites (Figure 6c), which, however, incurs more signaling storms for *static* users due to LEO satellites' extreme mobility (§3.2).

(3) Vulnerability to failures/attacks: Stateful procedures are vulnerable to intermittent satellite failures (from radiation and unreliable wireless links in Figure 13) and malicious attacks (e.g., satellite jamming, hijacking, man-in-the-middle attacks [36–40]). Pushing stateful core into satellites are also at the risk of sensitive state leakages (e.g., security keys).

3.1 Session Establishment

To use data services, the UE should first establish a session with the infrastructure. This session is stateful to enforce carrier-grade services and involves signaling exchanges between core functions. Session establishment is frequent for each UE (every 106.9s [43]) since inactive connections will be released after 10–15s for power saving [75] (thus later session re-establishments). In LEO networks, this procedure suffers from bottlenecks from space-terrestrial asymmetry.

Stateful sessions in terrestrial networks: Today's mobile network enforces carrier-grade services on a per-session basis between a UE and its fixed anchor gateway. Each session has five categories of states according to standards [45–50]: (1) *S1: identifiers*, including the UE and session identity; (2) *S2: UE locations*, including the UE's service area IDs (cell ID and tracking area ID) and IP address; (3) *S3: QoS*, including the QoS class, priority, and traffic forwarding rules; (4) *S4: Billing*, including the network usage report rules; and (5) *S5: Security*, including keys, authentication vectors, and access control policies.

Figure 10a–b shows procedures for the initial registration and session establishment. When the UE registers to 5G for the first time, AMF authenticates the UE and notifies SMF with QoS/billing profiles. Then the SMF selects a UPF as the anchor gateway to form a session. Later, to send uplink data, the UE first establishes a radio connection with the base station. Then the base station sends a service request to AMF, which copies the data session states to the base station for QoS enforcement. To deliver downlink traffic to an inactive UE, the anchor gateway should notify AMF on the data arrival. Then AMF notifies the base station to run paging for the UE. If successful, the device repeats the above procedure

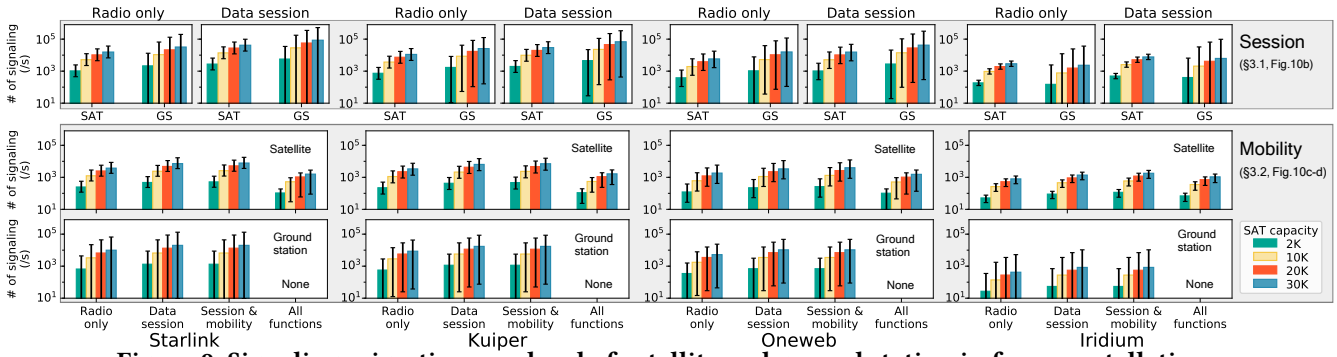


Figure 9: Signaling migration overhead of satellite and ground station in four constellations.

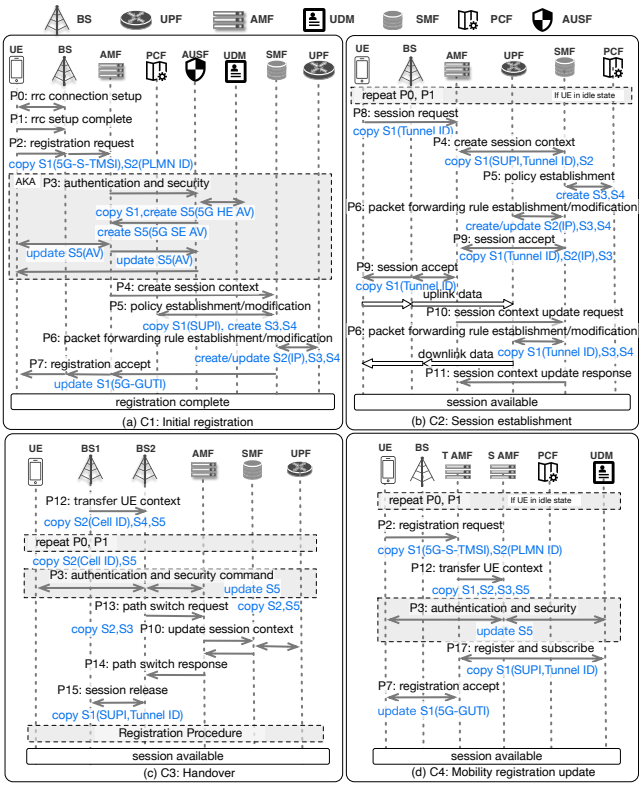


Figure 10: Terrestrial 5G signaling procedures [45–50].

to establish the session. From the state management perspective, these procedures synchronize session states between the UE, base station, and core network functions.

Bottlenecks from space-terrestrial asymmetry: Stateful sessions in space experience bottlenecks at the data and control plane. At the data plane, each session is coupled to a remote anchor gateway on ground. As shown in Figure 5a and §2.2, this anchor gateway becomes the single-point bottleneck since the global users' traffic from satellites would be redirected to it. At the control plane, session establishment incurs signaling exchange between network functions. If LEO satellites only have radio or session functions (Figure 6a–6b), they need to fetch session states from ground stations (P6/P9 in Figure 10b) and incur signaling overhead. Due to the space-terrestrial asymmetry and satellite routing, such signaling overhead will aggregate at satellite links and

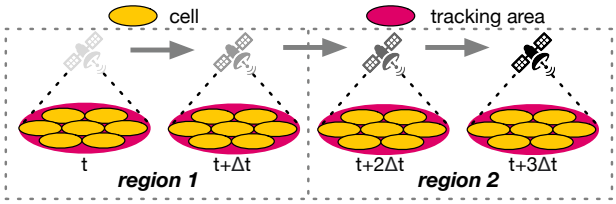


Figure 11: Moving service areas in satellite mobility.

ground stations, thus forming signaling storms. While moving AMF to satellites (Figure 6c) can avoid this issue in static scenarios, this option incurs even more state migrations in satellite mobility and offsets its merits, as we will see in §3.2.

Validation: Figure 9 shows the cost of session establishments in satellites and ground stations in Option 1 and 2 in Figure 6. For each satellite, the session establishment incurs 1,035–41,559 signaling messages/s depending on the satellite's maximal user capacity. For each remote ground station, signaling messages of session establishments from all satellites is up to an order of magnitude larger than satellites' signaling cost due to space-terrestrial asymmetry. Option 3 and 4 do not suffer from this deficiency but experience more deficiencies as we will show below.

3.2 Infrastructure Mobility from Space

Unlike fixed terrestrial infrastructure, orbital core network functions experience extreme mobility from LEO satellites (up to 7.6 km/s, Table 1). While the legacy core natively supports seamless *user mobility* functions, it requires fixed infrastructure (as anchors) and cannot support *infrastructure mobility*. If placed into fast-moving LEO satellites, the legacy stateful mobility functions will trigger *fast-moving service areas* and thus exhaustive signaling costs for even *static* UEs.

Stateful mobility control in terrestrial networks: The legacy mobile network tracks a UE's location and services by its service area IDs (S2 in §3.1). As the UE moves to a new service area (cell/tracking area), its session states in §3.1 should be migrated to the new service area to retain continuous services. Figure 10c–d illustrates how this works between fine-grained cells (via handovers) and coarse-grained tracking areas (via mobility registration). In handovers, the old base station migrates its session states to the new base station via AMF or direct tunnels. In mobility registrations, the device reports its arrival to the new location to the new AMF.

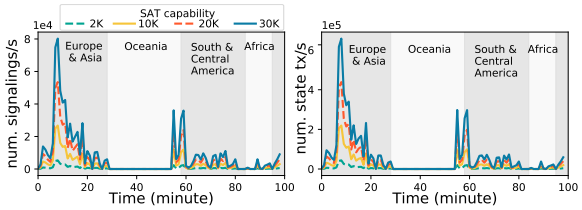
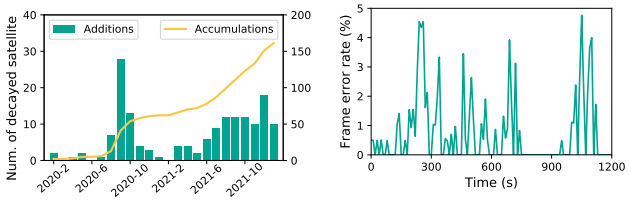


Figure 12: Temporal dynamics of a fast-moving LEO satellite's signaling overhead in Option 3 (Figure 6c).



(a) Satellite failures (Starlink [34]) (b) Radio link failures (Tiantong)

Figure 13: Intermittent failures in mobile satellites.

The new AMF migrates states from the old AMF, after which the old AMF deletes the states. The new SMF updates the session and possibly gateways to resume data service.

Moving service areas for static users: The legacy mobile network design binds its service area ID (cell/tracking area ID) its *logical* function node IDs (base station/AMF) on the premise that they are fixed anchors. While feasible for terrestrial infrastructure, such logical service areas would be unstable if pushing mobility functions to LEO satellites. As shown in Figure 11, as a logical base station or AMF, a satellite will result in fast-moving "cells" and "tracking areas". Note each LEO satellite only has transient coverage (≈165.8s in Starlink) for its 1,000s–10,000s of terrestrial users. These static users have to initiate procedures in Figure 10c–d and trigger signaling storms for satellites and ground stations.

Validation: Figure 9 compares the cost of mobility events. If only radio functions are in space (Option 1-2), LEO mobility triggers 248–7,169 (662-19,927) handover messages/s for each satellite (ground station) depending on each satellite's capacities in Starlink. With mobility functions in space (Option 3–4), the mobility registrations are also triggered and result in 105–7,801 (1,324-19,927) signaling messages/s for each satellite (ground station). As exemplified in Figure 12, such signaling overhead is *bursty* as static users in the same area simultaneously enter an incoming satellite's coverage. It also varies over time as each satellite traverses different global locations. Both exhaust satellites' CPUs (Figure 7) and delay all users' mobility registrations by queuing (Figure 8). This signaling cost is amplified between neighboring satellites without direct links (due to opposite moving directions at polars). This results in multi-hop (up to 48) signaling traffic delivery with more latencies and bandwidth costs.

3.3 Resiliency in Harsh Foreign Space

Unlike fixed terrestrial infrastructure with isolations and protections, mobile LEO satellites are unavoidably exposed to unreliable, untrusted global locations with intermittent failures and malicious attacks. All stateful procedures in §3.1–3.2 are vulnerable to both threats and thus threatened by sensitive state leakages and failures (out of services).

Resiliency in terrestrial stateful core: The resiliency of the terrestrial mobile network mainly relies on the premise of *trusted, untampered, and reliable* infrastructure. Most terrestrial infrastructure nodes are fixed and fully controlled by the operator. They are isolated from external entities via dedicated hardware, IPsec-protected domains [50], private clouds, or public clouds with high security/availability (≥99.999% [76]). They are assumed to store, update, and migrate all states in §3.1 in a secure and reliable environment. Without this assumption, all procedures in Figure 10 can be insecure (e.g., user authentication vector or key leakage) or unreliable (e.g., signaling loss/error to block the entire procedures).

Why not resilient in space: The above premise in terrestrial mobile networks does not hold for LEO satellites in unreliable, untrusted outer space. If pushed to satellites, stateful functions in Figure 6 will suffer from two threats:

- *Satellite failures:* LEO satellites are prone to failures from radiation and debris in outer space. As shown in Figure 13a, every 1 out of 40 Starlink satellites may have failed since they use commodity CPUs without hardening against radiations [33, 34] (for cost reasons). Moreover, all satellite links are wireless and thus prone to intermittent disconnections (e.g., out-of-alignment for laster satellite links in mobility, and atmospheric attenuation for space-ground radio links [77] as exemplified in Figure 13b from our datasets). All procedures in Figure 10 are prone to these failures since any signaling message loss/error can block the entire procedure.
- *Satellite attacks:* Attacks for satellites have been hardly news (e.g., see [38] for a review). When exposed to foreign locations, satellites face hijacking [36, 37], man-in-the-middle passive listening [40], jamming [38], or physical attacks [39] by terrestrial nodes or satellites from adversarial countries. Stateful functions in these LEO satellites should maintain sensitive states (e.g., authentication vectors in Option 3–4, and permanent keys in UDM in Option 4) from numerous users and traverse globally (Figure 12), thus at the risk of leakages to adversaries. Jamming satellite links can also block the stateful procedures in Figure 10 and disrupt services.

Implications for proactive state management: Recent efforts seek to optimize the mobile core network functions by pre-fetching user states (e.g., authentication vectors in UAVs [41]) or proactively replicating/broadcasting them among nearby nodes [41–43]. These optimizations excel for terrestrial mobile networks in well-protected areas with superior performance. Unfortunately, they are at the risk of security context leakages if used by LEO satellites. We thus seek alternative secure, scalable, and performant cores in space.

4 A CASE OF STATELESS ORBITAL CORE

To solve issues in §3, we make a case for *stateless, decentralized, lightweight* mobile core network functions in space. If achievable, this paradigm could mitigate bottlenecks from space-terrestrial asymmetry, exhaustive state migrations from LEO satellite mobility, and state failures/attacks in the unreliable, untrusted foreign environments. The challenge is to retain carrier-grade services for traffic delivery, mobility, QoS, billing, and security after the function-state decoupling.

Our solution, SpaceCore, copes with this challenge with the following insight: *The devices naturally form a distributed state repository for core functions in satellites.* After registering to the home network (Figure 10a), a UE has replicated and stored its session states by itself. These states are locally accessible to new satellites to enable carrier-grade services for this UE, thus avoiding exhaustive multi-hop state migrations from home (§3.1). They remain local despite LEO satellite mobility, thus preventing unnecessary invocations of procedures for user mobility in §3.2. They are not exposed to foreign locations and resilient to failures/attacks (§3.3).

Figure 14 overviews SpaceCore. It consists of the remote terrestrial home, LEO satellites as decentralized cores, and UEs. The terrestrial home is a legacy mobile core and runs all control functions, thus retaining operators' full control. The decentralized satellites push data functions and gateways from remote ground stations to edge, thus eliminating bottlenecks from space-terrestrial asymmetry in §3.1. SpaceCore decouples session states from data functions in satellites. Satellites directly fetches states from local UEs during the session establishment or mobility events. We next elaborate on SpaceCore's state-function-location decoupling (§4.1) and how its benefits procedures in Figure 10 in space (§4.2–4.4).

4.1 State-Function-Location Decoupling

SpaceCore enables stateless satellite core via *localized, geospatial state management*. It takes three steps. First, SpaceCore decouples the basic concept of service areas (cells/tracking areas) in legacy mobile network designs from the fast-moving LEO satellites. It shifts from today's *logical* service areas to *geospatial* ones, which remain stable in satellite mobility. Next, SpaceCore simplifies most location states in §3.1 and unifies a UE's logical and physical locations. Last, SpaceCore delegates satellite core' other states to local UEs, thus forming a distributed geospatial local state repository[4]. Any authorized stateless satellite that enters a service area can serve its UEs with local states. We next explain each step.

Step 1: Geospatial service area-satellite decoupling. Recall the legacy mobile network tracks a UE's location and service by its service area (cell/tracking area). In the terrestrial

[4]We note 5G also has an infrastructure-side state repository (UDSF [78, 79]), which is slow [80] and suffers from issues in §3 in satellites (Figure 7).

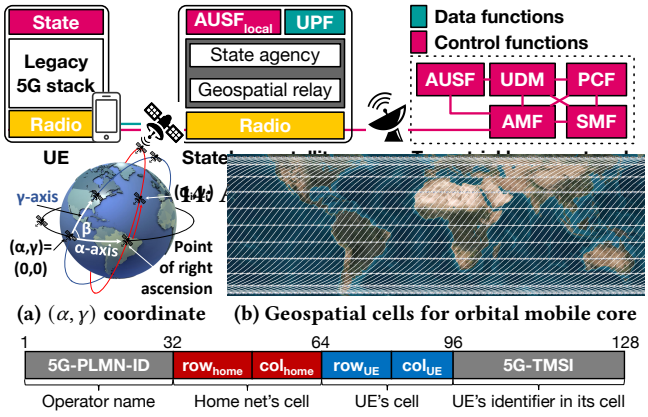


Figure 15: SpaceCore's geospatial service area & state.

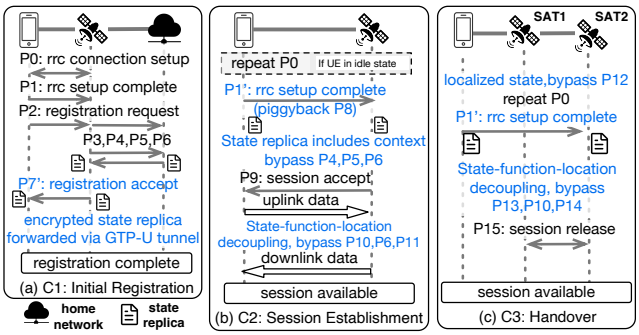


Figure 16: Localized state management in space (C4 is eliminated by geospatial mobility management).

mobile network, each cell (tracking area) is tightly coupled and identified by the fixed anchor base station (AMF) and remains stable. But in LEO mega-constellations, this design causes moving service areas in satellite mobility (Figure 11), incurs exhaustive state migrations for even static UEs (§3.2), and thus complicates the state management.

To this end, SpaceCore decouples cells/tracking areas from the fast-moving satellites. It redefines a cell/tracking area as a *geospatial* area, rather than a logical area identified by a functional node (e.g., satellite). This ensures each cell/tracking area remains stable despite satellites' extreme mobility.

Figure 15 showcases SpaceCore's geospatial cell division for LEO mega-constellations in Table 1. Unlike most geospatial systems (latitude/longitude, Google S2 [81] or Uber H3 [82]), SpaceCore defines its cells based on LEO constellations' orbital parameters to facilitate data session, mobility, and security functions in satellites (detailed in §4.1). As shown in Table 1, Most operational LEO constellations (Starlink, Kuiper, and OneWeb) are *uniform*: Each constellation has m circular orbits (all with inclined angle β) that are uniformly spanned across the Equator. Each orbit has n satellites that are uniformly placed on this orbit. For such a uniform LEO constellation, we define an affine spherical coordinate system in Figure 15a. Each terrestrial location is uniquely identified by a coordinate (α, γ), where α is the classical latitude and γ is a generalized *inclined longitude* as the angular distance

	Num. satellites	Min. cell size (km^2)	Max. cell size (km^2)	Avg. cell size (km^2)
Starlink	1,584	93,382	1,616,366	471,476
Kuiper	1,296	116,716	1,685,950	526,697
OneWeb	720	336,294	4,508,080	1,573,215

Table 3: SpaceCore's cells in real LEO constellations.

on a great circle with inclined angle β. At the constellation initialization ($t = 0$), SpaceCore projects all satellites' initial location to the earth and connects them along the (α, γ) coordinate system. Since then, SpaceCore uses this inclined grid cell division in Figure 15b as the fixed geospatial cells (with totally 72×12 cells). Then SpaceCore tracks a UE's location and service by its geospatial cell in Figure 15b.

Step 2: Simplify location states (S2). Once decoupled from the geospatial cells, the fast-moving LEO satellites no longer need to track a UE's location and service, thus eliminating most internal logical location states (cell/tracking area IDs) in §3.1. Instead, SpaceCore only keeps an UE's IP address as its location state, but redefines its addressing scheme to unify the UE's logical and physical location. As shown in Figure 15c, SpaceCore's geospatial IP address is a concatenation of new prefix, hierarchical geographical ID, and the UE suffix. The prefix is used for networking with external networks. The per-UE suffix ensures the globally unique address inside each cell. A UE's address remains fixed unless it moves to a new cell (which is rare due to the cell size in Table 3).

Step 3: Delegate other states to local UEs. For other states (S1, S3–S5), SpaceCore delegates them from LEO satellites to the local UEs. This results in a stateless satellite core and a *distributed geographical state repository by local devices*. Most of these states are readily available in UEs today once registered to the core network (Figure 10a). They are locally stored in UEs and thus free of exhaustive state migrations (§3.1–3.2) or leakage (§3.3) in satellite mobility. In the following, we elaborate on how it enables localized state management for the data sessions, mobility control, and security.

Step 4: UE-assisted local state management. With UEs as distributed state repositories, SpaceCore localizes state management for session establishments, mobility, and security functions in Figure 10 to address the concerns in §3. We next describe how SpaceCore achieves so for each procedure.

4.2 Localized Session Establishment

SpaceCore localizes most session establishments from space and mitigates single-point bottlenecks from the remote home (§3.1). Its core idea is that, after registration for the first time, each UE has locally replicated the states in §3.1 from the home. It can assist satellites in establishing local sessions for carrier-grade services *without* redirecting to the home.

Initial registration: Each UE follows the standard procedure in Figure 10a for the authentication, security key agreement, state creations, and session setup with the remote terrestrial home. In this process, the home network retains

Algorithm 1 Stateless geospatial relaying in Grid+ topology.

Input: The satellite's runtime location $S = (\alpha_s(t), \gamma_s(t))$, coverage radius ΔS[5], and distance to its neighboring satellites $\Delta\alpha$, $\Delta\gamma$
Output: The next hop for a data packet destined to $D = (\alpha_d, \gamma_d)$

```
if α_d ∈ [α_s − ΔS, α_s + ΔS] and γ_d ∈ [γ_s − ΔS, γ_s + ΔS] then
    Run paging and forward packet to D; return;   ▷ The satellite covers destination
else if |α_d − α_s| > |γ_d − γ_s| then
    if (α_d > α_s and α_d − α_s > m/2·Δα) or (α_d ≤ α_s and α_s − α_d ≤ m/2·Δα)
    then next_hop=S.left; end if                  ▷ Forward to left neighbor
    if (α_d > α_s and α_d − α_s ≤ m/2·Δα) or (α_d ≤ α_s and α_s − α_d > m/2·Δα)
    then next_hop=S.right; end if                 ▷ Forward to right neighbor
else
    if (γ_d > γ_s and γ_d − γ_s > n/2 · Δγ) or (γ_d ≤ γ_s and γ_s − γ_d ≤ n/2 · Δγ)
    then next_hop=S.down; end if                  ▷ Forward to bottom neighbor
    if (γ_d ≤ γ_s and γ_d − γ_s ≤ n/2 · Δγ) or (γ_d ≤ γ_s and γ_s − γ_d > n/2 · Δγ)
    then next_hop=S.up; end if                    ▷ Forward to upper neighbor
end if
return next_hop;
```

full control for each UE's data forwarding, QoS, billing, and security by generating session states based on these policies. After the successful registration, the home network allocates the geospatial IP address in Figure 15c to the UE, encrypts these states based on its satellite access control policies (detailed in §4.4) and delegates them to the local UE.

Uplink session establishment: This procedure is invoked when the UE wants to send data but has no active radio connection to its serving satellite. Its legacy workflow in Figure 10b incurs state copies and data relays with the remote terrestrial home network, both causing bottlenecks due to space-terrestrial asymmetry and triangular routing (Figure 5). Instead, SpaceCore leverages the UE's state replica to localize the session establishment. As shown in Figure 16a, the UE piggybacks its state replica to its serving LEO satellite during the radio connection setup (which can be readily achieved by reusing UE's AT commands, as detailed in §5). If authorized to access these local states by the home network (detailed in §4.4), the serving satellite can successfully decrypt and install them into its local radio access and UPF functions for immediate data services. Otherwise, the serving satellite fails to decrypt these states and rolls back to the legacy procedure in Figure 10b by contacting the home network.

Downlink session establishment: This procedure occurs when a UE should receive its data but has no active radio connection to satellites. Compared to the uplink case, the new challenge is how satellites can deliver this UE's data to the correct location *without* maintaining UE's location states. To avoid single-point bottlenecks in §3.1, SpaceCore pushes data services to edge satellites and removes the fixed anchor gateway (Figure 5). But without this anchor, the network has no reference point to relay the data to the fast-moving edge satellite covering the UE at runtime, notify the UE to set up the radio connection via paging, and deliver the data.

To this end, SpaceCore adopts stateless data forwarding between satellites by *geospatial cells*. In §4.1, we decouple the geospatial service areas from fast-moving satellites and embed the UE's geospatial cell into its IP address. By comparing

the destination UE's address and its runtime location, each satellite can estimate its physical distance to the destination and decide the next-hop satellite. Algorithm 1 shows how it works for the state-of-the-art grid satellite network topology. Each satellite has 4 links (2 for intra-orbit neighbors, and 2 for inter-orbit neighbors). Forwarding packets through each hop results in a *constant* $\pm\Delta\alpha$ (for inter-orbit links) or $\pm\Delta\gamma$ (for intra-orbit links) physical distance traversal in SpaceCore's (α, γ) coordinate system. Therefore, Algorithm 1 selects the physically closest next-hop satellite to forward data. If the current satellite has covered the destination UE, it runs paging to notify the UE. Then the UE repeats the procedure in Figure 16a to set up downlink services with its local states.

Analysis: SpaceCore offers three merits for session establishments in space: (1) *Performance:* SpaceCore removes the single-point bottleneck from the remote terrestrial home network (Figure 5) and speeds up the session establishment via local state operations; (2) *Scalability:* SpaceCore mitigates state migrations between satellites and the home network (§3.1); (3) *Resiliency:* By localizing the session establishment, SpaceCore prevents sensitive state leakages. After successful registration, SpaceCore can retain services even with unreliable inter-satellite links or intermediate satellite failures.

4.3 Geospatial Mobility Management

SpaceCore shifts to *geospatial location-based* mobility management by decoupling the service areas from fast-moving satellites (§4.1). It avoids unnecessary state migrations in satellite mobility (§3.2) and retains the legacy functions for UE mobility. We next describe how SpaceCore achieves so in handovers and mobility registrations.

Handovers by satellite mobility: A static UE in the idle mode (i.e., no active radio connections) does not experience handovers as satellites move. Even if the static UE reselects the satellite, no state updates are needed because SpaceCore decouples geospatial cells from satellites and adopts Algorithm 1 for successful paging and data delivery.

A static UE with active radio connections may face two types of handovers: (1) *Beam handover*, where the UE switches from one antenna to another from the same satellite. This occurs at the physical layer without core state operations; (2) *Inter-satellite handover*, in which the UE switches from one satellite to another. The new satellite should install the UE states to retain seamless ongoing data services. The standard handover achieves so by migrating the old satellite's states to the new satellite, which suffers from multi-hop delivery in satellite networks (§3.2). Instead, SpaceCore offers another option with UE's local states (Figure 16): Once switching to the new satellite, the UE piggybacks its state replica in the handover acknowledgment message to the new satellite. This results in an equivalent but shorter state migration path.

No mobility registrations by satellite mobility: Unlike legacy stateful designs, SpaceCore eliminates track area updates due to moving satellites. This is because SpaceCore decouples geospatial tracking areas from satellites (§4.1). A static UE's tracking area remains unchanged regardless of its serving satellite and is thus free of updates. In this way, SpaceCore avoids exhaustive state migrations in §3.2.

Handovers/mobility registrations in UE mobility: Both only occur if the UE crosses geospatial cells (uncommon due to large cell sizes in Table 3). In this case, the UE should update its location to the remote terrestrial home. The home follows the standard procedure in Figure 10d to re-authenticate the UE, re-allocate its geospatial IP address, and possibly update QoS/billing states based on the new location's policies (e.g., roaming in new countries). The UE will receive an updated state from home for later services in this cell.

Analysis: SpaceCore eliminates unnecessary handovers and mobility registrations in satellite mobility, thus scalable and performant in LEO satellite mobility. It also reduces the state migrations between satellites and thus the risks of attacks (e.g., state leakages) or failures (traversing fewer intermittent wireless satellite links and space-ground links).

4.4 Home-Controlled State Updates

Mobile networks may need to enforce dynamic QoS or billing policies (e.g., "unlimited data speed for the first 15GB data, and throttled to 128Kbps afterward") for some UEs. We support this with home-controlled state updates. In SpaceCore, the home is the only entity that can update all states except S2 and S5. It receives the dynamic data usage reports from the remote satellites, runs its policy control functions, and updates session states to the local UE and serving satellites using the session modification procedure. For S2, the UE notifies its new locations to the home network if it moves to the new geospatial cell (§4.3). Local state updates by UEs or satellites are prohibited (except S2 and S5) since states have been signed by the home network (detailed below).

Meanwhile, to mitigate sensitive security state leakages (S5 in §3.3), SpaceCore delegates most authentication and key agreements to local UEs and edge satellites. The legacy mobile network's security relies on symmetric key-based shared secret states [50]. Instead, SpaceCore's stateless design implies UEs and satellites should establish a mutual trust *without* mutual states. Therefore, it adopts public-private key cryptography[6] for local security and state protection with home-controlled attributed-based encryption (ABE [83, 84]). It allows the home to specify the access control policies based on UEs and satellites' attributes, thus resilient to unauthorized state access or modifications by local UEs/satellites.

[6]We note 5G has also adopted public-private key cryptography to encrypt user identity (SUCI) in the initial registration to protect user privacy [50].

Algorithm 2 Home-controlled local mutual authentication.

Initialization:
  Home: (pk, msk)←Setup(1^λ); ▷ *Master key initialization*
  Home → Satellite: CERT_{sat},sk_{sat}←KeyGen(pk, msk, S_{sat});
  Home → UE: sk_{UE}←KeyGen(pk, msk, S_{UE}); ▷ *Pre-stored in SIM card.*
Initial registration (C1):
  Home: state_{UE} ←(ver, TTL, IP, QoS, billing, p, g); ▷ *State initialization*
  Home → UE: msg_{UE} ←Encrypt(pk, state_{UE}, $\mathbb{A}$); ▷ *Encryption by policy*
  UE: state_{UE} ←Decrypt(msg_{UE}, sk_{UE}); ▷ *Keep state until TTL expiry*
Later service establishments (C2–C3): ▷ *Piggybacked in connection setup*
  UE → Satellite: X← $g^x \mod p$, msg_{UE};
  Satellite: state_{UE} ←Decrypt(msg_{UE}, sk_{sat}); ▷ *Successful if* $\mathbb{A}(S_{sat})$*=true*
  Satellite: Y←state_{UE}.$g^y \mod \text{state}_{UE}$.p, K←$X^y \mod \text{state}_{UE}$.p;
  Satellite → UE: Y, CERT_{sat};
  UE: Verify(CERT_{sat}, pk_{sat}), K←$Y^x \mod p$;

Algorithm 2 shows SpaceCore's local authentication, key agreement, and state access. At the initialization, the home network prepares secret key pair (pk, msk), generate keys for authorized satellites (UEs) based on its attribute sets S_{sat} (S_{UE}), and install them to satellites (before their launches to space) and UEs (in SIM cards). For the first-time registration (C1), the UE and home network follow the legacy protocol in P3 in Figure 10a for mutual authentication. In this process, the home encrypts the UE states with its private key pk and an access tree structure $\mathbb{A}$ (in the form of a Boolean formula). $\mathbb{A}$ is specific to this UE with $\mathbb{A}(S_{UE})$=true and defines the satellites' access control policies. For example, $\mathbb{A}(S)$ = {(S is UE **and** S.SUPI==UE.SUPI) **or** (S is satellite **and** S supports QoS **and** S.bandwidth≥10Gbps)}. For later services (C2–C3 in Figure 16), the UE and its serving satellite runs local authentication and key agreement by verifying their states/certificates. Note the satellite can successfully decrypt the UE's states if and only if its attributes satisfy the home's access control policy ($\mathbb{A}(S_{sat})$=true). Otherwise, the satellite rolls back to the legacy procedure in Figure 10. In Appendix A, we analyze Algorithm 2 and show it retains the same security as the legacy terrestrial mobile network.

5 IMPLEMENTATION

Figure 14 shows SpaceCore's deployment in 5G. For backward compatibility, we realize SpaceCore as an external proxy for the legacy 5G functions. This proxy is implemented with the readily available features in commodity UEs, satellites, and terrestrial infrastructure. The terrestrial 5G core can be extended as SpaceCore's home network, thus facilitating seamless space-terrestrial mobile network integration.

• **Satellites:** LEO satellites run the legacy 5G radio, UPF, and SpaceCore proxy. At the control plane, the SpaceCore proxy follows §4.1–4.4 to fetch and decrypt states from local UEs upon legacy 5G requests (P1, P2, and P8 in Figure 16). If unsuccessful (e.g., no UE-side support or decryption failure), it rolls back to legacy 5G procedures in Figure 10 by relaying signaling messages to the remote home network. At the data plane, the SpaceCore proxy activates local radio paging in 5G [49, 85] (thus avoiding paging from remote AMFs at home), realizes Algorithm 1 using the satellites' switching or routing, relays packets to the upper-layer legacy UPF to enforce QoS/billing, and piggybacks UE states in the Future-ExtensionField (FEF) in the 5G GTP-U tunnel header [86, 87] for packets to the next-hop UPFs in the same session.

• **UEs:** SpaceCore can be realized in today's commodity UEs without hardware or 5G standard changes. It runs a local state proxy as a system app in commodity UEs. At the initial registration, the SpaceCore proxy stores the UE states from the home network. For later session establishments, the proxy leverages 5G's standard UE-initiated PDU session setup request [47] to piggyback local states to the satellites, as shown in Figure 16a. The proxy initiates this procedure with local UE states via AT+CGQREQ command [88], which is piggybacked in the RRC connection setup complete message (thus saving signaling and round trips). The satellite-side SpaceCore agency re-intercepts this message to extract local UE states and runs procedures in Figure 16.

• **Terrestrial home:** SpaceCore reuses terrestrial mobile core as its home network for seamless space-terrestrial integration. The operator just connects the existing terrestrial mobile core with the satellite ground stations, update its IP address allocation policy to satellite UEs based on geospatial cells (§4.1), and add support for policy-based UE state encryption (§4.4). Each UE uses the same identity to register to the space and terrestrial mobile network, and seamlessly switch between them via mobility registration in Figure 10d.

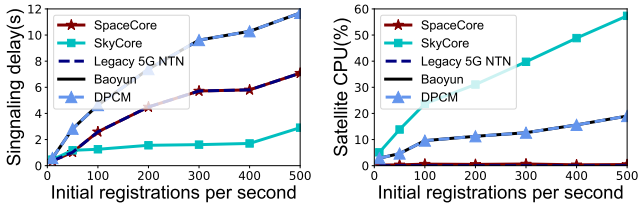
6 EVALUATION

We assess and compare SpaceCore with existing satellite 5G scenarios state-of-the-art satellite 5G optimizations.

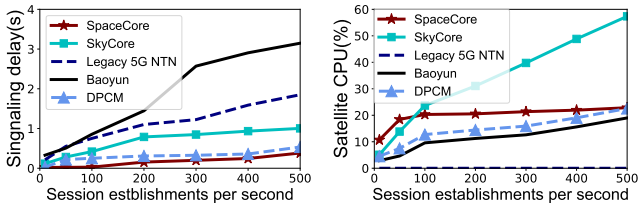
Experimental setup: We first validate SpaceCore's functionality in a small prototype (§6.1), and then assess it in LEO mega-constellations via large-scale emulations driven by operational 5G and satellites traces (§6.2).

◦ *Satellite and 5G dataset:* As shown in Table 2, we collect over-the-air signaling messages between operational geostationary satellites and three terrestrial satellite terminals (Figure 4b): Inmarsat Explorer 710 satellite terminal [89] (based on 3G UMTS [5, 54]), China Telecom's Tiantong SC310 satellite terminal [90] and T900 satellite phone [91] (2G GMR [4, 92]). For each device, we enable the diagnostic mode for its satellite baseband, and collect signaling messages of radio resource control (RRC), mobility management (MM), and session management (SM) protocols. We also collect over-the-air 5G signaling messages from China Unicom, China Mobile and China Telecom with Xiaomi 10/11 and OnePlus 9 running MobileInsight [70] with our extensions support these signaling message collections.

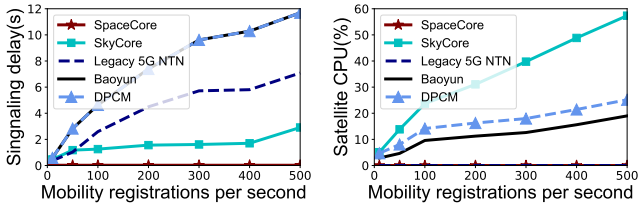
◦ *Testbed:* We follow §4–5 to prototype SpaceCore with open5gs [44] and OpenABE [93] on two hardware: (1) Raspberry Pi 4 used by Baoyun 5G LEO satellite [22, 29] and; (2)



(a) Initial registration



(b) Session establishment



(c) Mobility registration (by LEO satellite mobility)

Figure 17: Prototype results in hardware platform 1.

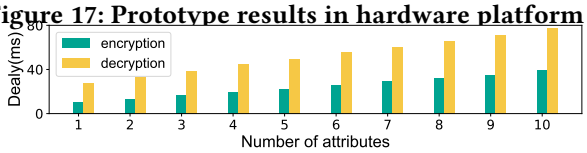


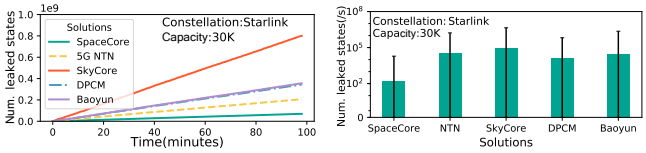
Figure 18: SpaceCore's local state processing costs.

Precision 7920 Workstation with Xeon E5-2630 (20 cores, 2.2GHz), which is similar to (weaker than) Hewlett Packard Enterprise EL 8000s (24 cores, 2.4GHz) used by OrbitsEdge in satellites [28, 74]. To assess SpaceCore at scale, we run SpaceCore in LEO mega-constellations in Table 1 (based on real orbital information from Space-Track [94]) and ground stations in [72] by replaying the above satellite/5G datasets.

6.1 Prototype Evaluation

We first examine SpaceCore's functionality in a small network with a home running full-fledged 5G protocol stacks in a ThinkStation P910, a SpaceCore satellite with Raspberry Pi 4, and terrestrial UEs emulated by UERANSIM [95]. We initiate procedures in Figure 10 and 16 with varying number of users to evaluate SpaceCore's performance and cost.

We compare SpaceCore with four satellite solutions: (1) **Legacy 5G NTN [15, 16]**, which is the *baseline*. We evaluate its regeneration mode (Figure 6a); (2) **SkyCore [41]**, which is the representative non-terrestrial mobile core (currently for UAV). It precomputes and stores all users' security contexts and policies in UAV/satellite to minimize state transfers from the ground, and proactively synchronize states between UAVs via broadcast. (3) **Baoyun [23]**, which is the first 5G core in real LEO satellites (Figure 4a and 6c); (4) **DPCM [43]**, which leverages device-side state replica to accelerate the



(a) Satellite hijacking (b) Man-in-the-middle (No IPsec)

Figure 19: Leaked sensitive states in satellite attacks.

	5G NTN	SkyCore	DPCM	Baoyun
Starlink	122.2×	17.5×	40.3×	49.3×
Kuiper	87.7×	19.3×	33.8×	42.8×
Oneweb	49.8 ×	20.1×	6.8×	25.8×
Iridium	34.5×	25.8×	7.7×	16.7×

Table 4: SpaceCore's satellite signaling cost reduction.

legacy signaling procedures (Figure 6c). Figure 17 shows the signaling delays and satellite CPU usages in these solutions.

• **Initial registration:** SpaceCore follows the legacy 5G in this scenario to retain reasonable delay and negligible satellite CPU (§4.2). SkyCore has the lowest latency since it has pre-stored all states to localize the initial registration, but at the cost of satellite CPU and security state leakages (§3.3). Baoyun and DPCM have the highest latency due to their interplays with the terrestrial home, and their in-orbit functions slow down the satellite processing (Figure 7).

• **Session establishment:** SpaceCore localizes it with UE-side states and achieves the lowest latency (§4.2). It is slightly faster than DPCM due to its lighter satellite CPU with fewer functions (mostly used by its attribute-based state decryption for security enforcements in §4.4, as quantifies in Figure 18). Instead, while SkyCore also localizes this procedure, its heavy functions in satellites slow down its processing. Meanwhile, other solutions require interplays with remote ground stations and thus incur long delays.

• **Mobility registration by LEO mobility:** SpaceCore eliminates this unnecessary procedure with its geospatial mobility management (§4.3), thus achieving negligible delays and satellite CPU costs. Instead, other solutions still suffer from such signaling costs due to the logical service areas.

6.2 Emulation in LEO Mega-Constellations

We next evaluate SpaceCore's scalability, performance, and resiliency with large-scale emulations in LEO satellite mega-constellations and ground stations. We run SpaceCore in LEO mega-constellations in Table 1 (based on real orbital information from Space-Track [94]) and ground stations in [72]. We assume the LEO mega-constellations use the grid satellite topology [6, 73] with inter-satellite traffic delivery capability. We run UERANSIM [95] with SpaceCore to emulate global mobile subscriptions statistics [71] and replay signaling datasets in Table 2 to trigger their signaling procedures. We repeat this experiment in SpaceCore and other solutions in §6.1 under varying LEO satellite capacities. Figure 20 shows the signaling costs without failures/attacks, and Figure 19 shows the resiliency to satellite attacks.

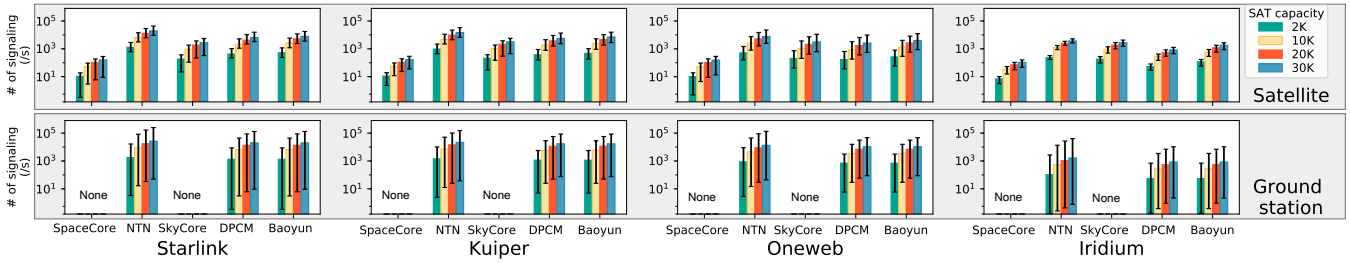


Figure 20: Signaling migration overhead per satellite and per ground station in five solutions.

Scalability: SpaceCore's localized, geospatial state management significantly saves the signaling costs. SpaceCore reduces 122.2×, 17.5×, 40.3×, and 49.3× signaling costs for satellites compared to 5G NTN, SkyCore, Baoyun, and DPCM, respectively in Starlink where capability of satellite is 30,000 users. By pushing data-plane functions to edge satellites, SpaceCore eliminates the remote ground stations's performance bottlenecks due to space-terrestrial asymmetry. By shifting to geospatial service areas, SpaceCore also saves the signaling costs from mobility registrations, and avoids state synchronizations between satellites (e.g., in SkyCore).

Performance: As shown in Figure 17, SpaceCore's lightweight, localized state management reduces 889 ms (6.90×), 1,529 ms (11.15×), 139 ms (1.92×), and 477 ms (4.16×) signaling delays in session establishment compared to the legacy 5G NTN, Baoyun, DPCM and SkyCore, respectively.

Resiliency to attacks/failures: Figure 19 shows the state leakages under satellite hijacking and man-in-the-middle passive listening of wireless inter-satellite links. SpaceCore is resilient to satellite hijacking due to its stateless nature; only the active serving users' keys are leaked in this case (which is unavoidable and can be counter-measured by disabling this satellite's access control, detailed in Appendix A). For comparison, other solutions leak more authentication vectors and keys due to proactive state replication or state migrations with remote terrestrial home. SpaceCore is also resilient to link failures and man-in-the-middle attacks since it localizes most state operations with few migrations. Other solutions may leak states during the migration since backend encryption (IPsec) is not mandatory in standards [50]. Enabling encryptions can mitigate man-in-the-middle attacks, but still cannot mitigate state leakages in satellite hijacking.

7 DISCUSSION

On radio access network (RAN): Our study focuses on mobile core functions and assumes standalone local RAN functions for each satellite (consistent with current 5G satellites [19–21]). This may be extended if, for example, future satellites adopt O-RAN/C-RAN [96–99] to split stateful radio functions. Similar state management issues would also occur and SpaceCore's general lessons can be generalized to RAN.

Implications for 6G and beyond: This study is based on the current 5G. While 5G has started to extend its support for satellites, its architecture is unlikely to change dramatically due to backward compatibility requirements (which results in our SpaceCore design). Looking forward, we believe a native stateless architecture in 6G and beyond would be necessary to unleash the potentials of LEO mega-constellations.

Will mobile networks win this space race? Besides mobile networks, there are other options for satellite networks, such as DTN [100], IP [73, 101, 102], MPLS [103, 104], DVB-S [105], CCSDS [106], to name a few. Which one will win this space race is beyond this paper's scope. Instead, this paper uses mobile networks to showcase the challenges of stateful functions in space. Its lessons are generally applicable to other network architecture and stateful functions as well.

8 RELATED WORK

Mobile networks are experiencing a technical leap due to the recent global 5G deployments and function openness to academia and industry. For radio access, extensive studies have been made based on O-RAN/C-RAN for function split [96, 97] and resource optimizations [98, 99]. For core networks, recent work refines core functions and state managements for low-latency access [42, 43], Internet-of-Things [69], UAVs [41], programmable core [107], cloudified function [76], network democratization [64], to name a few. Our study complements these efforts by exploring core network function redesigns in LEO satellite mega-constellations.

Enabling mobile network functions in space is still at the early stages. Despite being the *de facto* for satellite communications for decades [4–9], mobile networks have not migrated their core functions to satellites (§2.2) until the emergence of LEO mega-constellations in 2018. Recent LEO satellites from Lockheed Martin [19], Lynk [20], AST [21] (as radio access), China Mobile, and Huawei [22–24] (as core) have demonstrated the feasibility of enabling mobile network functions in a *single* satellite. Our work takes one step further to explore scalable, performant, and resilient mobile core functions in networked LEO mega-constellations.

9 CONCLUSION

This work explores the feasibility of enabling mobile core functions in low-earth-orbit mega-constellations. We show today's stateful mobile core suffers from LEO satellites' extreme mobility and exposure to unreliable, insecure outer space. This motivates us to make a case for SpaceCore, a stateless mobile core in space. SpaceCore decouples states from orbital core functions, reduces state migrations by shifting

to geospatial service areas, and localizes state management with device-as-the-repository for fewer failures/attacks.

In a broader context, SpaceCore simplifies stateful core network functions *for* the devices and *by* the devices. Since its origin, the mobile network has followed the infrastructure-centric design with heavy signaling and states. This method becomes expensive when infrastructure must move in harsh outer space. We hope our lessons can inspire and stimulate user-centric, lightweight mobile networks in the space era.

REFERENCES

[1] China makes big investments in 5G. http://english.www.gov.cn/news/topnews/202107/25/content_WS60fca12bc6d0df57f98dd886.html, Jul 2021.

[2] LightReading. China aims to drive down 5G power cost. https://www.lightreading.com/asia/china-aims-to-drive-down-5g-power-cost/d/d-id/765140, Nov 2020.

[3] ITU Publications. Measuring digital development: Facts and figures 2021. https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2021.pdf, 2021.

[4] ETSI. TS 101 376-1-3: GEO-Mobile Radio Interface Specifications; Part 1: General specifications; Sub-part 3: General System Description, 2009.

[5] ETSI. TS 102 744-3-6: Satellite Earth Stations and Systems (SES); Part 3: Control Plane and User Plane Specifications; Sub-part 6: Adaptation Layer Operation, 2015.

[6] Sydney Finkelstein and Shade H Sanford. Learning from corporate mistakes: The rise and fall of iridium. *Organizational Dynamics*, 29(2):138–148, 2000.

[7] OneWeb constellation. https://www.oneweb.world/, 2021.

[8] Inmarsat satellite communications. https://www.inmarsat.com/.

[9] FierceWireless. Inmarsat combines satellite and 5G for new type of network. https://www.fiercewireless.com/5g/inmarsat-combines-satellite-and-5g-for-new-type-network, 2021.

[10] Paolo Chini, Giovanni Giambene, and Sastri Kota. A survey on mobile satellite systems. *International Journal of Satellite Communications and Networking*, 28(1):29–57, 2010.

[11] Thuraya Telecom. https://thuraya.com/.

[12] SpaceX Starlink. https://www.starlink.com/, 2021.

[13] Amazon receives FCC approval for project Kuiper satellite constellation. https://tinyurl.com/bs7syjnk, 2020.

[14] FCC 21-115. Boeing: Application for Authority to Launch and Operate a Non-Geostationary Satellite Orbit System in the Fixed-Satellite Service. https://docs.fcc.gov/public/attachments/FCC-21-115A1.pdf, Nov 2021.

[15] 3GPP. TR38.811: Study on New Radio (NR) to support non-terrestrial networks, 2020.

[16] 3GPP. TR38.821: Solutions for NR to support non-terrestrial networks (NTN), 2020.

[17] 3GPP. Technical Specification Group Meeting #91E. https://www.3gpp.org/ftp/tsg_ran/TSG_RAN/TSGR_91e/Inbox/RP-210915.zip, Mar 2021.

[18] Qualcomm. On NR NTN Evolution. In *3GPP TSG RAN Rel-18 workshop*, 2021. https://www.3gpp.org/ftp/tsg_ran/TSG_RAN/TSGR_AHs/2021_06_RAN_Rel18_WS/Docs/RWS-210011.zip.

[19] FierceWireless. Lockheed Martin teams up with Omnispace on hybrid 5G space network. https://www.fiercewireless.com/5g/lockheed-martin-teams-up-omnispace-hybrid-5g-space-network, 2021. Video demo available: https://www.youtube.com/watch?v=MgK0ndOWJF0.

[20] SatelliteToday. Lynk Co-Founder Says Satellite-to-Cell Tech Will Be "Bigger than 5G". https://tinyurl.com/2p9a3an8, 2021.

[21] AST SpaceMobile. https://ast-science.com/spacemobile/, 2021.

[22] SpaceNews. Dongfang Hour China Aerospace News Roundup 6–13 December. https://spacewatch.global/2021/12/spacewatchgl-column-dongfang-hour-china-aerospace-news-roundup-6-13-december/, Dec 2021.

[23] Shangguang Wang, Qing Li, Mengwei Xu, Xiao Ma, Ao Zhou, and Qibo Sun. Tiansuan constellation: An open research platform. http://sguangwang.com/PDF/TiansuanFinal1203.pdf, 2021. The video demo is available at https://youtu.be/xECjZ1XBdWc.

[24] SpaceNews. Chinese private firm Galactic Energy puts five satellites in orbit with second launch. https://spacenews.com/chinese-private-firm-galactic-energy-puts-five-satellites-in-orbit-with-second-launch/, Dec 2021.

[25] Hughes. OneWeb Gateways Require Complex Hughes Engineering. https://www.hughes.com/resources/blog/satellite-essential/oneweb-gateways-require-complex-hughes-engineering, 2021.

[26] Inigo Del Portillo, Bruce G Cameron, and Edward F Crawley. A Technical Comparison of Three Low Earth Orbit Satellite Constellation Systems to Provide Global Broadband. *Acta Astronautica*, pages 123–135, 2019.

[27] 5G-Advanced core experiments in the Baoyun LEO Satellite by China Mobile. https://m.c114.com.cn/w118-1183668.html, Dec 2021.

[28] Oliver Peckham. Spaceborne Computer-2 Makes HPE's Case for Edge Processing. https://www.hpcwire.com/2021/09/02/spaceborne-computer-2-makes-hpes-case-for-edge-processing/, 2021.

[29] Raspberry Pi in space. https://www.raspberrypi.com/news/raspberry-pi-in-space/, Sep 2019.

[30] Lockheed Martin. Enhancements to NR-NTN and IOT-NTN in R18. In *3GPP TSG RAN Rel-18 workshop*, 2021. https://www.3gpp.org/ftp/TSG_RAN/TSG_RAN/TSGR_AHs/2021_06_RAN_Rel18_WS/Docs/RWS-210186.zip.

[31] Debopam Bhattacherjee, Simon Kassing, Melissa Licciardello, and Ankit Singla. In-orbit computing: An outlandish thought experiment? In *Proceedings of the 19th ACM Workshop on Hot Topics in Networks*, pages 197–204, 2020.

[32] Bradley Denby and Brandon Lucia. Orbital edge computing: Nanosatellite constellations as a new class of computer system. In *Proceedings of the Twenty-Fifth International Conference on Architectural Support for Programming Languages and Operating Systems*, pages 939–954, 2020.

[33] BusinessInsider. About 1 in 40 of SpaceX's Starlink satellites may have failed. https://www.businessinsider.com/spacex-starlink-internet-satellites-percent-failure-rate-space-debris-risk-2020-10, Nov 2020.

[34] Celestrak. Statistics of decayed Starlink satellites. https://tinyurl.com/56hktwy4, 2021.

[35] James Pavur and Ivan Martinovic. On detecting deception in space situational awareness. In *Proceedings of the 2021 ACM Asia Conference on Computer and Communications Security (AsiaCCS)*, pages 280–291, 2021.

[36] Wired. The Air Force Will Let Hackers Try to Hijack an Orbiting Satellite. https://www.wired.com/story/air-force-defcon-satellite-hacking/, Sep 2019.

[37] DefenseOne. Fearing Satellite Hacks and Hijacks, White House Issues Space-Security Directive to Industry. https://tinyurl.com/2p93wb2n, Sep 2020.

[38] Jacob G. Oakley. *Cybersecurity for Space: Protecting the Final Frontier*. Apress, 2020.

[39] TheVerge. China complains to UN after maneuvering its space station away from SpaceX Starlink satellites. https://tinyurl.com/ycyhr2ja, Dec 2021.

[40] Chunxiao Jiang, Xuexia Wang, Jian Wang, Hsiao-Hwa Chen, and Yong Ren. Security in Space Information Networks. *IEEE communications magazine*, 53(8):82–88, 2015.

[41] Moradi, Mehrdad and Sundaresan, Karthikeyan and Chai, Eugene and Rangarajan, Sampath and Mao, Z Morley. SkyCore: Moving Core to the Edge for Untethered and Reliable UAV-based LTE Networks. In *Proceedings of the 24th Annual International Conference on Mobile Computing and Networking (MobiCom)*, pages 35–49. ACM, 2018.

[42] Mukhtiar Ahmad, Syed Usman Jafri, Azam Ikram, Wasiq Noor Ahmad Qasmi, Muhammad Ali Nawazish, Zartash Afzal Uzmi, and Zafar Ayyub Qazi. A Low Latency and Consistent Cellular Control Plane. In *Proceedings of the Annual conference of the ACM Special Interest Group on Data Communication on the applications, technologies, architectures, and protocols for computer communication (SIGCOMM)*, pages 648–661, 2020.

[43] Yuanjie Li and Zengwen Yuan and Chunyi Peng. A Control-Plane Perspective on Reducing Data Access Latency in LTE Networks. In *ACM MobiCom*, Snowbird, Utah, USA, October 2017.

[44] Open5GS. https://open5gs.org/.

[45] 3GPP. TS23.501: System architecture for the 5G System (5GS), 2021.

[46] 3GPP. TS23.502: Procedures for the 5G System (5GS), 2021.

[47] 3GPP. TS24.501: Non-Access-Stratum (NAS) for 5G, Mar. 2021.

[48] 3GPP. TS38.413: NG Application Protocol, Oct. 2021.

[49] 3GPP. TS36.331: 5G NR: Radio Resource Control (RRC), Mar. 2021.

[50] 3GPP. TS33.501: Security architecture and procedures for 5G system, Sep. 2021.

[51] FierceWireless. Dish, RS Access lead new coalition in fight over 12 GHz band. https://www.fiercewireless.com/operators/dish-leads-new-coalition-fight-over-12-ghz-band, 2021.

[52] Andrew Jones. China kicks off a busy 2021 in space with communications satellite launch. https://www.space.com/china-launches-tiantong-1-03-communications-satellite, Jan 2021.

[53] Zizhong Tan, Honglei Qin, Li Cong, and Chao Zhao. New method for positioning using iridium satellite signals of opportunity. *IEEE Access*, 7:83412–83423, 2019.

[54] Broadband Global Area Network (BGAN). https://en.wikipedia.org/wiki/Broadband_Global_Area_Network, 2021.

[55] ZDNet. Verizon, Amazon's Project Kuiper team up on rural broadband, business connectivity. https://www.zdnet.com/article/verizon-amazons-project-kuiper-team-up-on-rural-broadband-business-connectivity/, 2021.

[56] Musk Sees Mobile Backhaul Future and CPE Equip Costs Cut in Half. https://www.telecompetitor.com/starlink-update-musk-sees-mobile-backhaul-future-and-cpe-equip-costs-cut-in-half/, 2021.

[57] KDDI selects SpaceX's Starlink for cellular backhaul. https://news.kddi.com/kddi/corporate/english/newsrelease/2021/09/13/5400.html, 2021.

[58] Yuanjie Li and Hewu Li and Lixin Liu and Wei Liu and Jiayi Liu and Jianping Wu and Qian Wu and Jun Liu and Zeqi Lai. "Internet in Space" for Terrestrial Users via Cyber-Physical Convergence. In *Twentieth ACM Workshop on Hot Topics in Networks (HotNets)*. ACM, 2021.

[59] Reddit. Online discussion with Starlink Engineers about satellites' capability. https://old.reddit.com/r/spacex/comments/gxb7j1/we_are_the_spacex_software_team_ask_us_anything/, 2021.

[60] Huawei. 5G Function Split Overview. https://tinyurl.com/3scu652d.

[61] 3GPP. TS38.211: 5G NR; Physical channels and modulation, Jun. 2019.

[62] 3GPP. TS38.212: 5G NR; Multiplexing and channel coding, Jun. 2019.

[63] 3GPP. TS38.213: 5G NR; Physical layer procedures for control, Jun. 2019.

[64] Zhihong Luo, Silvery Fu, Mark Theis, Shaddi Hasan, Sylvia Ratnasamy, and Scott Shenker. Democratizing cellular access with cellbricks. In *Proceedings of the 2021 ACM SIGCOMM 2021 Conference*, pages 626–640, 2021.

[65] Deepak Vasisht, Jayanth Shenoy, and Ranveer Chandra. L2d2: Low latency distributed downlink for leo satellites. In *Proceedings of the 2021 ACM SIGCOMM 2021 Conference*, pages 151–164, 2021.

[66] Intel. Intel Powers First Satellite with AI on Board. https://www.intel.com/content/www/us/en/newsroom/news/first-satellite-ai.html, 2020.

[67] DataCenterKnowledge. IBM Cloud Satellite Makes Your Data Center a Satellite of IBM Cloud. https://www.datacenterknowledge.com/ibm/ibm-cloud-satellite-makes-your-data-center-satellite-ibm-cloud, 2021.

[68] SpaceBelt Data Security as a Service. https://spacebelt.com/, 2021.

[69] Zafar Ayyub Qazi, Melvin Walls, Aurojit Panda, Vyas Sekar, Sylvia Ratnasamy, and Scott Shenker. A high performance packet core for next generation cellular networks. In *Proceedings of the Conference of the ACM Special Interest Group on Data Communication (SIGCOMM)*, pages 348–361, 2017.

[70] Mobileinsight. http://www.mobileinsight.net.

[71] World Bank. Mobile cellular subscriptions by country in 2019. https://ourworldindata.org/grapher/mobile-cellular-subscriptions-by-country, Jul 2021.

[72] Tesmanian. SpaceX Starlink Gateway Stations Found In The United States and Abroad. https://tinyurl.com/4m5uah43, 2021.

[73] Debopam Bhattacherjee and Ankit Singla. Network Topology Design at 27,000 km/hour. In *ACM CoNEXT*, 2019.

[74] OrbitsEdge: One Giant Step Towards Launch. https://orbitsedge.com/blog/f/one-giant-step-towards-launch.

[75] Arvind Narayanan, Xumiao Zhang, Ruiyang Zhu, Ahmad Hassan, Shuowei Jin, Xiao Zhu, Xiaoxuan Zhang, Denis Rybkin, Zhengxuan Yang, Zhuoqing Morley Mao, et al. A Variegated Look at 5G in the Wild: Performance, Power, and QoE implications. In *ACM SIGCOMM 2021*, pages 610–625, 2021.

[76] Binh Nguyen, Tian Zhang, Bozidar Radunovic, Ryan Stutsman, Thomas Karagiannis, Jakub Kocur, and Jacobus Van der Merwe. Echo: A reliable distributed cellular core network for hyper-scale public clouds. In *Proceedings of the 24th Annual International Conference on Mobile Computing and Networking*, pages 163–178, 2018.

[77] Yannick Hauri, Debopam Bhattacherjee, Manuel Grossmann, and Ankit Singla. "Internet from Space" without Inter-satellite Links? In *Proceedings of the 19th ACM Workshop on Hot Topics in Networks (HotNets)*, pages 205–211, 2020.

[78] 3GPP. TS29.598: 5G NR: 5G System; Unstructured Data Storage Services, Dec. 2021.

[79] 3GPP. TR29.808: Study on the Nudsf Service Based Interface, Dec. 2019.

[80] Umakant Kulkarni, Amit Sheoran, and Sonia Fahmy. The Cost of Stateless Network Functions in 5G. In *ACM/IEEE Symposium on Architectures for Networking and Communications Systems (ANSC'21)*, 2021.

[81] Google S2 geometry library. https://s2geometry.io/, 2021.

[82] H3: Uber's Hexagonal Hierarchical Spatial Index. https://s2geometry.io/, 2021.

[83] Shashank Agrawal and Melissa Chase. FAME: Fast Attribute-based Message Encryption. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS)*, pages 665–682, 2017.

[84] Vipul Goyal, Omkant Pandey, Amit Sahai, and Brent Waters. Attribute-based Encryption for Fine-grained Access Control of Encrypted Data. In *Proceedings of the 13th ACM conference on Computer*

and communications security, pages 89–98, 2006.
[85] 3GPP. TS25.301: Radio Interface Protocol Architecture, 2008.
[86] 3GPP. TS29.281: 3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service Tunneling Protocol for User Plane (GTPv1-U), year = 2021,, Sep.
[87] 3GPP. TS36.415: NG-RAN: PDU Session User Plane Protocol, Dec. 2021.
[88] 3GPP. TS27.007: AT command set for User Equipment (UE), 2011.
[89] Inmarsat Explorer 710 high-speed, portable BGAN terminal. https://www.cobhamsatcom.com/land-mobile-satcom-systems/ultra-portable-bgan/explorer-710/explorer-710-data-sheet/docview/, 2020.
[90] Tiantong SC310 satellite terminal. http://www.168jie.com/plus/view.php?aid=31, 2020.
[91] ZTE Tiantong T900 satellite phone. https://www.yoycart.com/Product/569970641057/, 2021.
[92] GEO-Mobile Radio Interface. https://en.wikipedia.org/wiki/GEO-Mobile_Radio_Interface, 2021.
[93] OpenABE. https://github.com/zeutro/openabe.
[94] Space Track. https://www.space-track.org, 2021.
[95] Ueransim. https://github.com/aligungr/UERANSIM.
[96] Open ran (o-ran) alliance. https://www.o-ran.org/.
[97] Nishant Budhdev, Raj Joshi, Pravein Govindan Kannan, Mun Choon Chan, and Tulika Mitra. FSA: Fronthaul Slicing Architecture for 5G using Dataplane Programmable Switches. In *Proceedings of the 27th Annual International Conference on Mobile Computing and Networking*, pages 723–735, 2021.
[98] Gines Garcia-Aviles, Andres Garcia-Saavedra, Marco Gramaglia, Xavier Costa-Perez, Pablo Serrano, and Albert Banchs. Nuberu: Reliable RAN virtualization in shared platforms. In *Proceedings of the 27th Annual International Conference on Mobile Computing and Networking (MobiCom)*, pages 749–761, 2021.
[99] Xenofon Foukas and Bozidar Radunovic. Concordia: Teaching the 5G vRAN to Share Compute. In *Proceedings of the 2021 ACM SIGCOMM 2021 Conference*, pages 580–596, 2021.
[100] Vinton Cerf, Scott Burleigh, Adrian Hooke, Leigh Torgerson, Robert Durst, Keith Scott, Kevin Fall, and Howard Weiss. Delay-tolerant networking architecture. 2007.
[101] Lloyd Wood, Will Ivancic, Dave Stewart, James Northam, Chris Jackson, and Alex da Silva Curiel. Ipv6 and ipsec on a satellite in space. In *58th International Astronautical Congress (IAC-07-B2.6.06)*, volume 2, page 810, 2007.
[102] Giacomo Giuliari, Tobias Klenze, Markus Legner, David Basin, Adrian Perrig, and Ankit Singla. Internet backbones in space. *SIGCOMM Comput. Commun. Rev.*, 50(1):25–37, 2020.
[103] FCC. Petition of Starlink Services, LLC for Designation as an Eligible Telecommunication Carrier. https://tinyurl.com/ury6rzw5, 2021.
[104] Amazon Kuiper mega-constellation. https://eurospace.org/wp-content/uploads/2020/11/information-note-amazon-kuiper_18112020.pdf, 2020.
[105] Dennis Roddy. *Satellite communications*. McGraw-Hill Education, 2006.
[106] Consultative Committee for Space Data Systems (CCSDS): All active publications. https://public.ccsds.org/publications/allpubs.aspx, 2021.
[107] Junguk Cho, Ryan Stutsman, and Jacobus Van der Merwe. Mobilestream: A scalable, programmable and evolvable mobile core control plane platform. In *Proceedings of the 14th International Conference on emerging Networking EXperiments and Technologies*, pages 293–306, 2018.
[108] 3GPP. TS33.401: Service requirements for the Evolved Packet System (EPS), Jun. 2016.
[109] Station-to-station protocol. https://en.wikipedia.org/wiki/Station-to-Station_protocol, 2021.

A SECURITY ANALYSIS

This section analyzes how SpaceCore ensures security with its local authentication, key agreement, and state verification in §4.4. We study SpaceCore's security under various threats, including state leakages/failures, authenticity, authorization, confidentiality, state integrity, man-in-the-middle attacks, replay attacks, and denial-of-service attacks. We show that (1) for threats that can be defended by the legacy mobile networks, SpaceCore should also defend it; (2) for threats that the legacy mobile network cannot defend, SpaceCore should not exacerbate them; and (3) SpaceCore does not create new security vulnerabilities.

Threat model: We follow the standard threat model for the mobile network [50, 108] but extend it in three aspects. First, we assume unreliable satellites that are vulnerable to intermittent wireless links and attacks in harsh foreign locations (§3.3). Second, we consider 3rd-party malicious satellites in outer space (e.g., from adversarial countries) that may actively fake as the legacy satellites or passively listen to the wireless links to intercept UEs and legacy satellites. Third, we assume *selfish UEs* that may attempt to manipulate SpaceCore's local states for their own merits (e.g., higher QoS or lower billing). We assume the home network is well-protected and trusted in the homeland.

UE state leakages/failures: SpaceCore is resilient to state leakages since satellites do not maintain permanent session states. Under satellite hijacking, only the current serving users' states may be leaked (which is unavoidable for any solutions). Its localized authentication also mitigates state migrations between satellites, thus more resilient to satellite node/link failures and man-in-the-middle passive listening by adversary satellites.

Authenticity: SpaceCore offers mutual authentication in the initial registration (Figure 10a) and Algorithm 2 based on UE's encrypted states (from home) and satellites' certificates. When a satellite is hijacked, the home network detects it and invalidates its authenticity by updating the access structure $\mathbb{A}$ and refreshing UEs' encrypted states such that $\mathbb{A}(S_{sat})$=false. In this way, hijacked satellites can no longer decrypt UEs' states to negotiate the keys according to Algorithm 2 (line 12).

Authorization: Algorithm 2 adopts the attribute-based encryption [83, 84] to let the home customize access control policies $\mathbb{A}$ for satellites (S_{sat}) and UEs (S_{UE}). This facilitates fine-grained access control based on QoS, billing, satellites and UEs' hardware capability, and other attributes.

ABE	Attribute Based Encryption
AKA	Authentication and Key Agreement Protocol
AMF	Access and Mobility Management Function
BS	Base station
CN	Core Network
CP	Control Plane
GEO	Geostationary Earth Orbit
GSL	Ground-Space Link
HN	Home Network
IMSI	International Mobile Subscriber Identity
ISL	Inter-Satellite Link
LEO	Low Earth Orbit
MEC	Multi-access Edge Computing
MM	Mobility Management
NAS	Non-Access Stratum
NTN	Non-Terrestrial Network
PCF	Policy and Charging Function
PDU	Protocol Data Unit
PLMN	Public Land Mobile Network
RAN	Radio Access Network
RRC	Radio Resource Control
SM	Session Management
SMF	Session Management Function
SUCI	Subscription Concealed Identifier
SUPI	Subscription Permanent Identifier
TMSI	Temporary Mobile Subscriber Identity
UDM	Unified Data Management
UDSF	Unstructured Data Storage Function
UE	User equipment
UPF	User Plane Function

Confidentiality: Algorithm 2 negotiates the security key K for signaling/data traffic encryption over the air and updates this security key for every session establishment (thus resilient to key leakages or satellite hijacking).
State integrity: Without the home network's key pair (pk, msk), neither the UE or satellite can fake or modify the states.
Man-in-the-middle attacks: Algorithm 2 negotiates the security key K based on the station-to-station protocol [109], which is resilient to man-in-the-middle attacks. The attacker cannot derive the keys K or decrypt the UE states by passively listening SpaceCore's message exchange.
Replay attacks: Without knowing the UE or satellite's secret keys sk_{sat}/sk_{UE} (pre-stored in trusted satellite hardware and UE's SIM), an attacker replaying the previous encrypted states cannot derive the keys K or decrypt the UE states. Moreover, each encrypted state is associated with a version number ver and time-to-live TTL. The home network can specify both fields to determine the lifetime of a UE-side state. On TTL expiry, the edge satellite will update states from the terrestrial home instead of using UE-side states (line 11 in Algorithm 2).
Denial-of-service attacks: The legacy mobile network is inherently vulnerable to DoS. The legacy mobile network [50, 108] decides not to fully address DoS due to the high cost. Similar attacks can appear in SpaceCore, but are not worsened by SpaceCore. Its signaling piggyback in §4.2 and 5 also mitigates signaling costs and thus DDoS attacks.